LogicMonitor

CASE STUDY

Henrico IT reduces alert noise by 90% with LogicMonitor

More than just “keeping the lights on”

HENRICO COUNTY
INFORMATION TECHNOLOGY

EMPLOYEES
5,100 (for Henrico general government and public libraries)

INDUSTRY
Government

BUSINESS GOALS

- Reduce alert noise and fatigue with tuned, actionable alerts
- More proactive monitoring to mitigate risk and improve customer experience
- Minimize downtime with 100% visibility across entire IT infrastructure and internal teams

SOLUTION
LM Infrastructure

BENEFITS

- Consolidated monitoring solutions and legacy tools within a single pane of glass for enhanced visibility
- Estimated 90% reduction in alert noise
- Prevented 4-5 outages by replacing SFPs or rebooting equipment

Introduction

County of Henrico’s IT team, like many other government IT teams, is responsible for keeping the lights on. But as many IT teams know, it’s rarely as easy as flipping a switch.

County of Henrico is a large region in central Virginia with roughly 350,000 residents. Henrico IT is comprised of IT Managers Rosario Gambardella, who oversees the System Administration and Infrastructure Group, Robert Aungst, who oversees the Network Infrastructure teams, and Reggie Grubbs, who oversees the previous teams as well as the Database group. Together, they are responsible for maintaining and monitoring the county’s entire IT infrastructure, in addition to offering infrastructure as a service for the county’s libraries and supporting emergency services (the 911 center, police department, and fire department).

The team manages more than 760 devices with various SaaS services, 40+ in house applications, two data center sites, a disaster recovery site with physical and virtual servers, Cisco and Meraki switches, routers, firewalls, and more. For most IT teams, including Henrico IT, the most important metric to track when monitoring this many devices is uptime.

Because County of Henrico supports the 911 center, police department, and fire department – services that could be life or death if their systems are down – maintaining consistent uptime is critical. The team monitors all network gear at fire stations, as well as supporting and monitoring the CAD (computer assistance dispatch) systems that the emergency response and 911 center heavily rely on. Unplanned downtime results in not only the inability to provide necessary services, but also potential capital losses, security vulnerabilities, and unhappy customers and users.

To successfully support the county’s infrastructure and offerings, including crucial emergency services, the team needed 100% visibility across their IT environment. The goal was to effectively predict any issue before they reached a critical status.

Gaining that visibility, however, was not always as easy as dialing 911.

Lost in the noise

A typical day for Aungst and his team starts with a 9am meeting. He checks in with his team, checks on their preliminary operational status, and creates a game plan for the day based on tuned alerts that require immediate attention.

With their previous monitoring solution, SolarWinds, that 9am meeting wasn't as smooth as it sounds. Building an action plan by looking at alerts was nearly impossible when Aungst and team were sifting through 5,000 alerts daily. In fact, Aungst's inbox was inundated with 25,000 alerts per week due to the lack of flexibility and customization offered by SolarWinds.

"It was noisy, not reliable, [and] alerts weren't actionable," said Grubbs. Even when SolarWinds' support team came on-site to help tune the platform to deliver what County of Henrico needed, "it still wasn't satisfactory."

On top of struggling to surface the most critical alerts in these massive alert storms, Henrico IT struggled with high overhead from having to run what Grubbs refers to as "beefy" servers on-premise to host their monitoring platform. They also struggled to delegate monitoring to their business units, which include infrastructure, database administration, applications, and development groups. The business owners of these units ensure that the infrastructure their applications run on is operating correctly and efficiently, while also ensuring public-facing web services stay online and accessible. With around 40% of their applications developed in-house, partnering with their application and development teams for monitoring efforts is essential.

The county's IT teams, particularly the team Gambardella oversees, needed to provide high-level monitoring insights to their business owners that would be most beneficial and actionable for the respective business units. With the alert structure from SolarWinds, providing actionable information was too difficult and often reactive. It only came with alert noise that constantly overwhelmed the teams and impacted overall operational efficiency.

Monitoring gaps and their impact

The team installed a cellular backup network for the fire stations they support to ensure minimal downtime with a dual link and multiple pathway approach. Previously, SolarWinds lacked the nuanced, granular view that would indicate when only one system or pathway went down. Instead, the team was only alerted when an entire router went down.

Being unable to detect when only one pathway went down meant the team had no insight into when a fire station defaults to a cellular network instead of a wired one. This monitoring gap can quickly turn costly, as running on a cellular network is significantly more expensive than remaining on a wired network. After a particularly high cellular bill came in unexpectedly, the team realized they didn't have the enhanced visibility or granular alerting required to cover this massive monitoring gap.

In order to obtain the required visibility to do their job effectively, it was time for Henrico IT to search for a new monitoring platform, preferably one with better visibility, tuned alerts, easy-to-use API, customization capabilities, and actionable insights. Cost savings would be a cherry on top.

Enter LogicMonitor

After highly publicized industry security concerns with their previous monitoring solution, Grubbs was ready to search for a new monitoring platform that worked for him and his teams.

“It really boils down to [this]: can we get it to perform the way we want it to and can we trust the alerts that we get now versus before. I mean that’s worth the price of admission right there,” said Grubbs. LogicMonitor’s SaaS-based, agentless solution, ease of use, intelligent alerting, and customization capabilities matched County of Henrico’s needs.

Aungst and team have seen an estimated 90% reduction in alert noise, with about three or four alerts per day, a huge drop in daily alerts from the 5,000 they experienced previously.

“For me, it’s no extraneous alerts. That’s the biggest thing, getting the alerts down to only stuff that’s actionable is fantastic. You can’t ask for anything better than that,” Aungst said. “In addition to that, the various DataSources like the EIGRP neighbors? You know that’s just something SolarWinds didn’t do.”

With LogicMonitor’s ability to monitor EIGRP neighbors and IGRP for their fire stations with dual links, the team can avoid any shocking cellular bills as the EIGRP neighbors only go down when the station is on the cellular network. “This gives us a clue that we need to troubleshoot the primary Comcast network instead, which is a wired network. The quicker we can get them back on the wired network, the less money they spend on cellular, so that’s a cost savings, too,” Aungst said.

The decrease in alert storms meant more proactive and predictive monitoring. With the ability to tune alerts for key information within their unique environment, Aungst explained that his team has seen four or five instances in the past couple of months in which they proactively prevented outages by replacing SFPs or rebooting equipment before disaster threatened to strike.

Without information fatigue clouding the business units, cross collaboration and operational efficiency have also been major wins for Henrico IT. The business units now have actionable alerts and no longer have to be the first ones to report any issues or outages to the IT Managers because they’re already on top of it.

“We’ve already gotten alerts that a particular link is down because an SFP was bad and they’ve lost half their bandwidth, for example. We create those tickets and act on it rather than the end users having to report it to us. It’s way more proactive and makes us look a whole lot better and that we know what we’re doing,” Aungst said.

Automation station

LogicMonitor’s automation and customization capabilities also stood out to the Henrico IT team during their search, and they’ve proved to be extremely beneficial. With LogicMonitor, Henrico IT replaced two existing monitoring tools: SolarWinds and MRTG. Previously, the team used MRTG for interface statistics, but that was a lengthy, manual process that required them to individually set up every interface, which LogicMonitor does by default.

County of Henrico’s libraries particularly love the visibility into their network uplinks to see how much bandwidth they’re using at any given time, while the IT team enjoys time for other tasks without the manual configuration required to set up those views.

LogicMonitor’s API also provided key customization capabilities, including a user-friendly way for Aungst to create his own Python script working off of LogicMonitor documentation. He can also now automate monitoring individual switch ports instead of clicking through each one to get his desired view. Since each stack contains eight switches and each switch contains 48 ports, this saves Aungst a lot of time.

Gambardella also had various application teams reach out, looking to integrate certain functionality from their applications – 40+ of them built in-house – with LogicMonitor.

“I’m not a code guy, so it’s easy to give them an API token to lay in their code and see whatever they need to. It’s all very straightforward,” Gambardella said. The customization of LogicMonitor’s DataSources was a huge win for Henrico IT’s teams, giving them the ability to bend the platform to their will. The team can now tweak any existing DataSources to see exactly what they want to see. They can also make those adjustments in a very user-friendly way, without waiting on a lengthy support process to implement their desired changes.

“It’s very nimble. I’ve had scenarios where particular DataSources weren’t included on a certain resource or something right off the bat, and I’ve been able to add that data for monitoring with ease to get the additional information I’m looking for,” Gambardella said.

Increasing operational efficiency and productivity

The IT Infrastructure Managers at County of Henrico have seen major improvements across multiple workflows with proactive alerting, allowing the team to get ahead of any major issues before a potential outage. They’ve also been able to delegate more monitoring directly to their business units, who were previously inundated with storms of unactionable alerts. Now that their business owners trust the alerting structure and capabilities with LogicMonitor, there has been an increase in requests for more monitoring, insights, and alerts for their respective areas of the business, increasing overall operational efficiency within the organization.

“That’s new to us. When we had SolarWinds, there wasn’t anyone really reaching out,” explained Grubbs. “Now that they know we have the capability with LogicMonitor and that it’s reliable and not just a lot of noise, I think they’re more receptive to getting those alerts directly.”

“It’s been a force multiplier as far as mission operations go. Not only do the system administrators or network administrators have oversight, but for the business units that we’ve delegated monitoring and reporting to, it’s spread the net basically,” Gambardella explained.

Henrico IT has also experienced an improved device onboarding process for new locations, whether that’s a new fire station coming online or a new county events center. The team already has everything they need tuned for fire stations, so when a new one comes online, set up is quick and efficient as they can easily go in under their designated group to find things they monitor. Active discovery has also been incredibly beneficial for quickly spinning up new environments, especially with their vCenter instance.

Finally, the days of excessive alert fatigue and letting important alerts slip through the cracks are over. Now, Aungst looks forward to his new morning routine.

“That’s how I start my day off: the first thing I look at is LogicMonitor,” he said.

Henrico IT will always be dedicated to keeping the lights on for their county and supporting services. But now with LogicMonitor’s automation, actionable alerts, enhanced visibility, and ease of use, Aungst, Gambardella, Grubbs, and their teams can sleep a little easier knowing that once that 9am meeting rolls around, they’ve got a game plan.