Case study
Cisco public

Mobile County Public School System Builds a More Secure Future with AMP for Endpoints

> **“Cisco AMP for Endpoints met our needs from all security standpoints. We’re seeing more and AMP is catching things that our previous endpoint protection didn’t catch. And AMP is saving us money; because it’s easier to run we can do more with less manpower.”**

George Mitchell Head of Research and Development, MCPSS

Established in 1836, the Mobile County Public School System (MCPSS) is the largest school system in Alabama with 7,500 employees comprised of teachers, staff, and administration. An IT department of nearly a dozen technicians, including three security professionals, handles everything that’s required from the endpoint to the network, from end user support to identifying and deploying new technologies. As George Mitchell, head of research and development for MCPSS says, “We’re an integral part of the heartbeat of the school system – there’s not a department we don’t touch.”

Executive Summary

Customer Name:
Mobile County Public School System (MCPSS)

Size:
7,500 employees

Deployment:
27,000 total endpoints
(PC workstations and laptops)

Industry: Education, K–12

Location: 89 schools across Mobile County, Alabama

“AMP brings Mobile County peace of mind because it’s a global product that keeps us safe from emerging threats and the vulnerabilities we couldn’t see before. We feel safer with Cisco AMP for Endpoints and look forward to building a more secure future for MCPSS.”

George Mitchell
Head of Research and Development, MCPSS

Better protection everywhere

As the threat landscape becomes more complex, protecting against malware while giving the teachers the flexibility they need to work from home safely is a chief concern. “Call it what you like – malware, viruses, phishing... we call it ‘extortionware’, and we deal with this every day; the bad guys are really crafty so you have to be craftier,” Mitchell explains. “We also have to provide protection everywhere – at school and offline too since our teachers have to bring their laptops home to work.”

Lack of integration between their existing endpoint security tools and other network and security systems also created challenges because the team had little visibility and control across MCPSS infrastructure. “Our systems weren’t interconnected so if you have a computer that is misbehaving, our previous endpoint protection might find the problem but it couldn’t shut the port down on the switch,” says Mitchell.

John Kennedy, hardware and network technician for the school district adds, “Without the ability to see and understand what was going on we could only be reactive. We’d get a virus or malware and there was really no way to figure out how it got onto the system. All we could do was react to what happened – we couldn’t do anything to prevent it from happening again.”

A more effective, simpler approach to security

MCPSS knew they needed to increase security as attacks accelerated and became more sophisticated, so they began to seek alternative solutions. “Because the world has changed, you can’t just sit there with an anti-virus product and that’s all it does,” says Kennedy. “We really needed something that could open up our eyes to problems in our system and help us answer the question of how viruses are getting in. If you don’t know, you can’t stop them.”

In addition to addressing their security challenges, the solution had to be cloud-based to reduce administration costs while optimizing performance. “With our previous solution, we had to update every workstation each time we wanted the latest protection. When you’re talking about nearly 30,000 machines, it’s time-consuming,” says Mitchell. “Users also don’t like having more software installed on their systems. It slows performance. The new solution had to be web-based.”

MCPSS also wanted to simplify management in order to eliminate the burden on their lean team and accelerate detection and response. “Integration between our endpoints and our network was important for us because when you have a security problem, you can deal with problems a lot faster – you’re not wasting time jumping between multiple consoles,” Kennedy explains. “We chose Cisco AMP for Endpoints because it met all these requirements.”

Up and running fast

"As a cloud-based software-as-a-service solution, AMP for Endpoints requires only a lightweight connector on endpoints. "Deployment really went smoothly," says Kennedy. "We literally got AMP for Endpoints out in production within two weeks, deploying it to 27,000 workstations without any problems."

The solution was also much simpler to manage than the previous solution. "I have one console to look at my entire system and know what the health is of my system and all of my workstations," says Kennedy. "I can quickly see all of my current security problems without having to scroll through a bunch of pages. AMP for Endpoints makes life a whole lot easier."

Gaining deep visibility into endpoint activity

AMP for Endpoints prevented breaches and blocked malware that MCPSS's previous solution was missing. "We started noticing the limitations of our previous endpoint protection solution and double-checked to make sure it was patched," Kennedy says. "If we had the latest version then why wasn't it detecting threats that AMP for Endpoints was detecting?"

Because no prevention method will catch every threat, AMP for Endpoints also provides deep visibility when an advanced threat gets inside the network. "We now have a lot more insight than we've had with any other solution in the past," shares Byron Lipscomb, network technician at MCPSS. "Cisco AMP for Endpoints not only gives us the post-mortem after infection, but also how the infection happened and who has been infected with the same files."

Kennedy adds, "It's like getting to see how a magic trick is performed. We can watch from the creation to the end result of what the virus did and its one of the capabilities I like the most. Instead of having to go back and try to figure out what the user did and how they did it, with file trajectory every time a file is copied, moved, or executed, AMP's watching. I can actually select on that file and block it on all my clients."

The MCPSS team has benefitted in additional ways from file trajectory – blocking the use of unauthorized software. "With increased visibility into non-virus related activity, we found out students were sharing a VPN software," Lipscomb explains. "Even though it wasn't detecting as a virus, file trajectory allowed us to track down which computer saw it first and block it."

Rapid time to detection

Adversaries move quickly once inside the network and can cause damage fast. "Nowadays, speed to detection of viruses is pretty critical because they can wipe out your entire system quickly," says Kennedy. "The faster you can detect it, the sooner you can prevent it."

Lipscomb describes one incident in particular. "We actually had an outbreak at one of our

"We now have a lot more insight than we've had with any other solution in the past. Cisco AMP for Endpoints not only gives us the post-mortem after infection, but also how the infection happened and who has been infected with the same files."

Byron Lipscomb
Network Technician, MCPSS

schools that our previous product didn't detect. At first it scared us, because we started getting thousands of hits. And once we dug in more, we saw that AMP for Endpoints was actually blocking it from starting."

Kennedy further explains, "We noticed that one of our workstations was generating almost 24,000 quarantines that Cisco AMP caught. Without AMP we would have been blind to what was going on – 24,000 viruses would have been spread had AMP not been doing what it's supposed to."

Automation also plays a critical role in helping this small team respond quickly and effectively to threats. "In the security world, we have to have automation because you're not sitting in front of a screen looking for something to happen," says Mitchell. "An outbreak can happen at any time – it might be at night or over the weekend. We have to have automated systems that detect, detain, and alert us."

Kennedy adds, "Cisco AMP provides automation – detecting a threat and shutting it off instantly so that when you get to work the next day you can deal with it. That, to us, is gold."

Protection on and off network

One of the challenges for the MCPSS team is ensuring devices are continuously protected. To address this, Cisco AMP for Endpoints provides both an offline and on-network engine. "We have close to 4,000 teachers and they're bringing their laptops and devices home," says Mitchell. "Cisco AMP for Endpoints has helped ensure that teachers and administrators remain protected wherever they go. The solution scans to make sure they aren't introducing a zero-day threat by detecting and stopping anything malicious before it can infect the network."

An integrated approach that's a force multiplier

In addition to Cisco AMP for Endpoints, the Mobile County Public School System also uses Cisco Identity Services Engine (ISE) for secure network access, Cisco Email Security, and Cisco Prime Infrastructure. "What helped us choose Cisco AMP was having all the right pieces working together seamlessly, helping us create a safer school system," says Mitchell. "With AMP on the endpoint talking to ISE we can shut down outbreaks before they happen."

An integrated approach also creates operational efficiencies. "Having all the Cisco products integrated really helps out with deployment times and help desk tickets," says Lipscomb. "If we're deploying switches to a new building, we simply put them on a deployment VLAN, Prime configures them for ISE, and they're set up. And as soon as somebody plugs in, it's instantly integrated with AMP to stop any viruses. It just works right off the bat."

Kennedy describes how integration helps drive increased visibility. "One thing we like about having software that's integrated is you can see

"I have one console to look at my entire system and know what the health is of my system and all of my workstations. I can quickly see all of my current security problems without having to scroll through a bunch of pages. AMP for Endpoints makes life a lot easier."

John Kennedy
Hardware and Network Technician, MCPSS

all the assets and what they're doing," Kennedy explains. "I don't have to close down one program and open up another program to see what's happening."

Mitchell adds, "We've also seen significant cost savings when we combine all our Cisco products: ISE, CES, AMP, and Prime. Using these solutions all together benefits our entire district as a whole. From cost savings to automation to integration to better security, it's a win-win situation for the Mobile County Public Schools System."

A more secure future

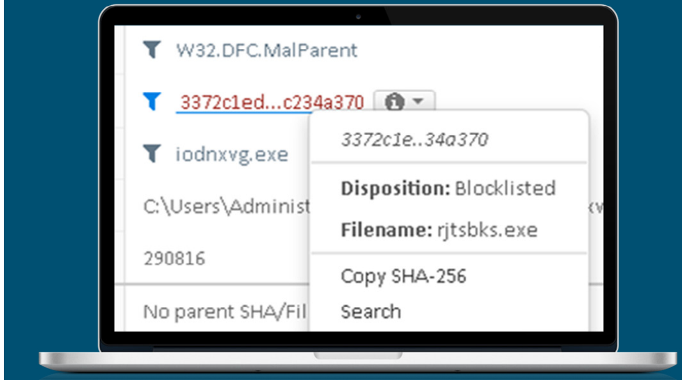
Mitchell is excited about a future that includes Cisco AMP for Endpoints as part of their integrated security architecture. "Cisco AMP for Endpoints met our needs from all security standpoints," says Mitchell. "We're seeing more and AMP is catching things that our previous endpoint protection didn't catch. And AMP is saving us money; because it's easier to run we can do more with less manpower."

"AMP brings Mobile County peace of mind because it's a global product that keeps us safe from emerging threats and the vulnerabilities we couldn't see before," adds Mitchell. "We feel safer with Cisco AMP for Endpoints and look forward to building a more secure future for MCPSS."

To learn more about Cisco AMP for Endpoints, visit www.cisco.com/go/ampendpoint

Products and Services

- Cisco Advanced Malware Protection (AMP) for Endpoints
- Cisco Identity Services Engine (ISE)
- Cisco Email Security
- Cisco Prime Infrastructure



W32.DFC.MalParent

3372c1ed...c234a370

iodnxvg.exe

C:\Users\Administ

290816

No parent SHA/Fil

3372c1e..34a370

Disposition: Blocklisted

Filename: rjtsbks.exe

Copy SHA-256

Search