

# Orchestrating the end of malware

Symphony achieves first-chair defense with Malwarebytes

## INDUSTRY

Nonprofit

## BUSINESS CHALLENGE

Prevent ransomware and malware infections with minimal IT intervention required

## IT ENVIRONMENT

McAfee antivirus, firewalls, Active Directory and group-based permissions

## SOLUTION

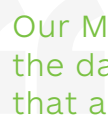
Malwarebytes Endpoint Security

## RESULTS

- Significantly reduced risk of malware and ransomware infections
- Simplified malware detection and response for small staff
- Eliminated malware-related disruptions for users

## Business profile

The San Francisco Symphony is one of the most successful and adventurous arts institutions in the U.S. It presents more than 220 concerts annually and reaches 600,000 people in Davies Symphony Hall, through education and community programs, and on national and international tours. When ransomware and malware struck, Malwarebytes helped re-harmonize users' endpoints.



Our McAfee solution just wasn't catching the dangerous malware and ransomware that are attacking us. Replacing it with Malwarebytes gives us the strong protection we need to stay secure.

—Aaron Bennett, Chief Information Officer,  
The San Francisco Symphony

## Business challenge

Stop ransomware and improve malware detection

"Today, we're fighting straight-up attempts at fraud," said Aaron Bennett, Chief Information Officer for the San Francisco Symphony. "Malware attacks are launched by people trying to get money, whether through ransomware, spoofing, or other means. Viruses no longer seem to be in vogue."

The Symphony had been using a McAfee antivirus, but it wasn't catching ransomware or malware. Fortunately, the organization's users are pretty sharp at recognizing unusual browser behavior and suspicious emails, and the IT team caught the first instance of ransomware quickly. But they knew that ransomware, malware, spoofing, and suspicious files were on the rise—and they needed better defense.

"After the first instance, I figured out what the file extension was and then literally looked for that extension on files on our servers," said Bennett. "Once we found it, we could see which system it was on. At that point, we'd remove the system from the network and reimage it."



Although Bennett's team used file utilities to search for ransomware and other malware on the servers, it was still time-consuming. And it would only search for files with the specific extensions that the IT team was looking for. New variants of malware or ransomware could potentially get through undetected.

"We wanted an enterprise-class, anti-malware solution with centralized management to detect and stop ransomware and malware," said Bennett. "After looking at several possible solutions, our desktop support engineer suggested Malwarebytes. We tried it, and we liked its usability. Most importantly, it worked."

## The solution

### Malwarebytes Endpoint Security

The Symphony chose Malwarebytes Endpoint Security and also subscribed to Malwarebytes Premium Support. Bennett says that the Malwarebytes support team shared best practices and offered his team options for deployment and configuration, spending valued time on the phone to help deploy the solution.

"Our McAfee solution just wasn't catching the dangerous malware and ransomware that are attacking us," said Bennett. "Replacing it with Malwarebytes gives us the strong protection we need to stay secure."

### Seeing every part

"Malwarebytes has a nice enterprise graphical interface that I can look at," said Bennett. "It's more intuitive than the antivirus solution was. We can see and track all of our systems. For instance, right now I look at the Management Console and see 384,000 threats."

Machines are quick-scanned daily and then scanned fully once a week. Malwarebytes eliminates malware that runs scheduled processes on a user's machine, which the antivirus solution could not do. Now, malware can no longer hide and multiply.

### Increasing the tempo of response

Malware threats are obvious to the Symphony's IT team through the Management Console. If a suspicious instance appears, the team can quickly troubleshoot and respond appropriately. The graphical interface clearly shows threats, endpoint status, and upgrades—everything the team needs to know at a glance.

"We don't have a large department or staff, so the solution had to be easy to use," said Bennett. "It is. We can quickly see who is compromised and what is attacking without a lot of clicking around."


### A threat diminuendo

With Malwarebytes, threats significantly decreased. Unlike signature-based antivirus solutions, Malwarebytes protects the Symphony against zero-day exploits and blocks malicious websites—and it does it all without slowing down users' machines.

"We're impressed with the amount of malware that Malwarebytes finds," said Bennett. "Not only does it give us peace of mind that we're catching this stuff, users aren't disrupted by malware-related incidents. It's like music to our ears."

## | About

Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company's flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts.

-  Santa Clara, CA
-  [malwarebytes.com](https://malwarebytes.com)
-  [corporate-sales@malwarebytes.com](mailto:corporate-sales@malwarebytes.com)
-  1.800.520.2796