Malwarebytes

CASE STUDY

California Department of Consumer Affairs prevents zero-day malware attacks

Malwarebytes tracks, blocks, and protects systems from repeated malware attacks

INDUSTRY
Government

BUSINESS CHALLENGE
Prevent recurring infections from malware

IT ENVIRONMENT
Data center with McAfee ePolicy Orchestrator, firewall, proxy services, email gateway, FireEye, Trend Micro TippingPoint security management system

SOLUTION
Malwarebytes Anti-Malware for Business

RESULTS
- Eradicated 99 percent of malware problems
- Reduced the number of machines re-imaged daily from 10 to zero, saving days of valuable staff time
- Stopped recurring malware infections

Business profile

The California Department of Consumer Affairs (DCA) works to protect California consumers from unsafe products and services, as well as from unscrupulous and unlicensed practitioners. To help make sure that consumers are protected, DCA licenses professionals and advocates consumer interests before lawmakers. But when it came to cyberthreats, DCA needed more than its current antivirus solution to protect its own interests from malware attacks.

> Malwarebytes gives us hands-free protection, which has allowed us to redirect staff to more strategic projects.
>
> —Jim Epp, Section Chief, OIS Client IT Support Services, California Department of Consumer Affairs

Business challenge

Stop recurring malware infections

DCA has 25 Office of Information Services (OIS) staff members that support 2,900 desktop and mobile computing devices. As cyberthreats increased, so did their toll on employees' workstations. Soon after DCA deployed a FireEye security solution, it began detecting odd traffic patterns between workstations. Some workstations suddenly showed a burst of network activity for no apparent reason. However, there were no clues that alerted users to anything unusual, and there was no remediation provided.

When that happened, the OIS team would go to the workstation, scan it with the McAfee antivirus solution, and inform McAfee. But the McAfee solution just couldn't keep up with zero-day attacks. Frequently, they also had to re-image the workstation, which took two to three hours each time. At first, they might have to re-image three or four infected machines a day. But as threats increased, at peak times they were re-imaging up to 10 machines a day.

Dealing with infected machines took at least three staff members away from other important projects. And it was disruptive to users,

especially those who had to send their systems to Sacramento from bureaus in other parts of California.

"What was so frustrating is that we'd get machines cleaned and within hours, FireEye again detected problems on those machines," said Jim Epp, Section Chief, OIS Client IT Support Services at DCA. "So we began looking for a solution to catch malware and zero-day threats, and we found Malwarebytes."

The solution

Malwarebytes Anti-Malware for Business

The OIS team tried Malwarebytes Anti-Malware for Business and immediately found a high number of malware problems that several layers of protection had missed. That was the solution they were looking for. After a fast, painless deployment, the difference was huge.

"With Malwarebytes deployed, we eradicated 99 percent of the malware problems we'd been having," said Epp. "Now my team uses the Malwarebytes Management Console to scan machines weekly, and users don't even notice."

Removing the unknown

"You can't effectively deal with unknown cyberthreats," said Baird Cowan, Chief Technology Officer at DCA. "With visibility from Malwarebytes, we not only know what is attacking us, we know why infections were recurring. They don't anymore."

Malwarebytes identified all of the usual malware suspects—command and control programs, bots, Potentially Unwanted Programs (PUPs), Trojans, and others lurking on department machines. Now, they can do something about it. Malwarebytes blocks attacks and enables the OIS team to trace them to a source. For example, if an infected machine connects to the network in a field office, the team can stop malware at the source and prevent it from infecting other machines at headquarters and at other bureaus over the network.

Strong addition to the security portfolio

"Malwarebytes complements everything we have to protect our systems," said Epp. "It gives us hands-free protection, which has allowed us to redirect staff to more strategic projects."

Malwarebytes saves days of time that used to be spent working on infected workstations and laptops. Epp can't remember the last time they re-imaged a machine because instances of malware getting through are so rare.

"We recently completed a security audit," said Epp, "and Malwarebytes has been a strong addition to our portfolio of tools. I expect that we'll continue to expand on its capabilities."

Supports the mission

The Department of Consumer Affairs' primary mission is to protect consumers and legitimate licensed professionals from unscrupulous businesses. An important part of that mission requires protecting clients' data.

"Malwarebytes gives us the ability to achieve our mission more easily and efficiently," said Cowan. "When we can protect our users, our systems, and client information, we can better protect California consumers. It's a win-win."

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

corporate-sales@malwarebytes.com

1.800.520.2796