CaseStudy: Community Action Committee of Pike County

How Comodo helps the Committee protect its IT infrastructure from malware and spam

CYBER SECURITY IS A CHALLENGE FOR EVERY SIZE COMPANY

The malware threats of today are being designed to hack into any size infrastructure and cause chaos -- stealing personal information, financial and corporate records, or planting infections to simply cause IT destruction.

All of these new threats start out as an unknown file. But with the onslaught of cyber-crime, the traditional antivirus blacklisting of files cannot keep up – and the lag time between malware being made public and then appearing on a blacklist is devastating to companies. Additionally, traditional antivirus solutions have focused on detection - not prevention – using default allow technology, which only stops recognized, blacklisted files.

But what if a file is unknown and doesn't appear on the blacklist? Then traditional antivirus technology allows it to enter an IT environment and potentially infect a system.

Technology that can recognize and contain an unknown file is paramount to the prevention of cyber-attacks and malware penetration.

For small business and non-profit organizations, IT needs are the same as large corporations – a safe IT environment that allows for the storage, collaboration and exchanging of information for the better of the company.

But for those small business and non-profit organizations, large IT staffs and budgets are not a standard practice, meaning they could possibly be the most susceptible to attacks. Community Action Committee of Pike County (CAC) is one such organization that wanted to ensure its IT environment was safe.

CAC is a non-profit organization dedicated to promoting self-sufficiency among the low income population of Pike County, and to address the major causes of poverty. Established in 1964, the organization offers a range of home weatherization assistance, consumer energy education, emergency home repair and handicapped accessibility modification programs. It operates several family health centers, serving the needs of individuals in southern Ohio.

APPROACH

The streamlined IT administration team at CAC consists of just 2 employees who are managing more than 350 computers and endpoints, 30 servers along with a variety of network equipment, across 14 locations. Without the budget of the average corporate entity, CAC needed to find a method of reducing the amount of time consumed by endpoint antivirus management, while at the same time ensure that its data was secure and contained from any threat of malware – all at a price point that would fit within the budget. CAC's technology infrastructure houses county financial information and budgets, as well as individual's social security numbers, finances, and home addresses – very personal information to its clients.

Key Features and Benefits of **Comodo Endpoint Security Manager**

- Standalone containerization complements and enhances any existing security solution to block unknown files from infecting an endpoint
- Award winning five layered defense in-depth suite (Antivirus, Firewall, Host Intrusion Prevention, Automatic Containment and File Reputation) built on Comodo's Default Deny architecture
- Deep dive analysis of managed endpoints operation through a single click and dashboard view
- Patent-pending containerization technology prevents zero-day malware attacks
- Smart filtering to automatically contain and execute unknown files, without negatively impacting system performance or the user's productivity

"We always have a number of concerns for our IT needs – keeping our very sensitive data secure, maintaining a IT system that is virus free, and managing multiple endpoints on a very streamlined budget," said Matthew Dill, IT Coordinator, Community Action Committee of Pike County.

SOLUTION

As CAC's current contract with Symantec was nearing expiration, the IT department looked at all competitive solutions on anti-virus and anti-spam to evaluate the best cost versus the best performance, to make its next IT infrastructure decision. Through its own research and previous experiences, CAC pulled in all the major vendors including McAfee, Symantec, and Comodo among others.

"We ran multiple tests and benchmarks of putting Comodo, Symantec and other anti-virus technologies against one other to simply pick out who would perform best," said Dill. "When we tested the Comodo endpoint security product, it detected viruses and malware that none of the other competing products detected. It was right then and there that we knew Comodo's technology had to be the new solution for us to protect our critical data."

The Comodo Endpoint Security Management (ESM) software suite brings five layers of defense (antivirus, firewall, host intrusion prevention, automatic containment and file reputation) right to the point of impact. Comodo's real-time automatic containment technology, which is part of Comodo ESM, eliminates malware outbreaks and operating system contamination by automatically running untrusted processes in an isolated environment.

"We strive to protect our clients' information across all programs within our agency and Comodo's antispam protection provides us with a tool that fulfills this need efficiently," said Meka McClay, IT Director, Community Action Committee of Pike County. "The Comodo Endpoint Security Manager enables us to perform a host of functions directly from the console, eliminating the need to physically connect to each machine. This allows us to complete our work without interrupting the user's workflow. We also like the remote access feature of this product."

"The Comodo technology works very well for our needs for our IT department. Comodo's sandboxing technology keeps us worry-free because it automatically contains any threat that might be made against our infrastructure," said McClay.

For IT administrators, as well as CIOs and CISOs who need to prevent data breaches, Comodo endpoint security is the only solution that offers on-device, real-time containment. Unlike legacy approaches such as blacklisting and sandboxing, Comodo endpoint security uses smart filtering to automatically contain and execute unknown files, without negatively impacting the system performance and the user's productivity.

ADDITIONAL INFORMATION

Learn more about the Community Action Committee of Pike County at **http://www.pikecac.org**

About Comodo

Comodo
1255 Broad Street
Clifton, NJ 07013
United States

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information. With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

For more information, visit **www.comodo.com**

COMODO
Creating Trust Online®