CaseStudy: Christian Motorcyclists Association

Organization Trusts Comodo's Advanced Endpoint Protection Technology to Stay Malware Free

Key Features and Benefits of **Comodo Advanced Endpoint Protection**

- Automated containerization, Comodo VirusScope behavior and action analysis
- Static, dynamic and human analysis with Comodo Valkyrie
- A multi-layered defense suite that includes host firewall, HIPS, Web URL filtering, file reputation, jailing protection, certificate-based whitelisting, and persistent VPN
- Unified management of Android, iOS, and Windows enabled devices
- Fully integrated device management, application management and device security
- Enterprise-wide visibility of all running unknown contained processes or executables
- Enterprise-wide, on-demand scanning for malware
- Patent-pending containerization technology which prevents zero-day malware attacks

ORGANIZATIONS LARGE AND SMALL NEED TO KEEP THEIR INFORMATION PROTECTED FROM THE UNKNOWN

Globally headquartered in Mena, Arkansas, the Christian Motorcyclists Association (CMA) is a non-profit, evangelistic organization which outreaches primarily, but not exclusively, to the motorcycling community. CMA's vision is "Changing the world, one heart at a time," a vision carried out with a servant's attitude to the world and to its members saying they are here if you need them.

CMA (http://www.cmausa.org/) celebrated its 40-year anniversary in 2015. What started in 1975 as one man on a motorcycle with a willingness to obey God has grown into a worldwide ministry with thousands of members and chapters across the USA and outreaches in more than 30 countries worldwide.

Like most organizations and companies across the world today, CMA keeps all of its critical information in the cyber world, through its network and computer systems. This includes confidential and restricted information like global and regional memberships, donation records, accounts receivable and payable, and additional confidential information only intended for the eyes of its members and affiliates.

CMA members and leadership are continuously using email, web portals and social media across landline, Ethernet and WiFi hotspots. All of this key information is utilized and leveraged by the leadership and IT team across its networks where it can be shared, collaborated on, and maximized by the teams, in the spirit of CMA's mission.

However, in an age of cyber criminals where social security numbers, financial records, and personal and business information all need to be protected and secured – companies and organizations are looking at new cyber security alternatives that focus on the prevention of attack, not just the detection when a virus or malware attack has happened. Fears of unknown malware attacks, such as zero-day and advanced persistent threats, have become some of the real world challenges for the System IT Administrators at CMA.

"Like any organization or business today, the Christian Motorcyclists Association is conducting all forms of business in the online world," said Clint Davis, IT Manager for CMA. "Our members, affiliates and leadership team members are staying in constant contact, sharing information across hundreds of endpoints about new donations or finances, organizational business, tax information and contracts - and they need to be assured that information that is supposed to stay in-house does just that."

CMA's main data center, which houses its critical information and business applications, was using a mixture of multiple antivirus and IT security detection solutions from various companies, but was still experiencing frequent infections and viruses. The IT team was encountering rogue malware, Trojans, and viruses across its network, and clearing an average of three major IT security infections per week. On top of what the IT team was finding, they lived with the reality that an unknown rogue piece of malware might be lurking in their network, one they had yet to find, one which no antivirus or security system they had in place could find – until it might be too late.

TURNING TO COMODO FOR ADVANCED ENDPOINT PROTECTION

With various endpoints and disparate IT security systems in place, CMA researched alternative cybersecurity companies that could deliver on two core needs for the Association: manageability of endpoints from a single console and the ability to protect endpoints from infection – both from known and new, unidentified threats.

Against these criteria, CMA evaluated Symantec,

Kaspersky, McAfee, Bitdefender, Trend Micro, Avast, and Comodo based on their own internal research to try and understand what would be the best option for their needs. In the end, Comodo Advanced Endpoint Protection was selected as the choice for CMA.

Comodo Advanced Endpoint Protection provides total protection against zero-day and advanced persistent threats while having no impact on CMA's end-user experience or any of their workflows. Any untrusted or unknown applications that are started by CMA's users are automatically contained in a secure environment, allowing all safe applications the freedom to run while denying all malware access to the system which they require to deliver their payloads, and attack an IT environment.

The Comodo Advanced Endpoint Protection solution is built upon a next generation, Default Deny platform which blocks and isolates unknown, zero day attacks of malware, spyware, Trojans and other harmful executables - and renders those attacks useless against endpoints and networks. Comodo has unified its endpoint security solution and enterprise class device management - including Comodo Endpoint Security Manager and Comodo Device Manager – into Comodo Advanced Endpoint Protection

The foundation of Comodo Advanced Endpoint Protection is Comodo Client, which includes antivirus, firewall, web URL filtering, host intrusion prevention, containment and file reputation, and Comodo ITSM, which allows for the configuration of the security policies and visibility into the security infrastructure of enterprise endpoints through solutions such as mobile device management and remote monitoring and management.

The Comodo ITSM dashboard is used by the IT team at CMA for panoramic insight and to control all aspects of endpoint protection and management. Its streamlined interface displays 14 critical metrics from all of the endpoints at CMA, facilitating rapid alerting and remediation of issues. CMA's IT System Administrators can also terminate endpoint processes, stop or start services, uninstall applications and delete unwanted files—all without causing any interference to the end user.

Comodo Advanced Endpoint Protection brings multiple layers of defense, including antivirus, firewall, web URL filtering, host intrusion prevention, auto-sandbox (containment), and file reputation together under a single offering for customers of all sizes, to protect them from both known and unknown threats. The Christian Motorcyclists Association has been running Comodo Advanced Endpoint Protection since early 2015 and has not experienced a single IT security issue to date.

"Compared to its competitor's offerings, Comodo did require some slight additional implementation configuration to identify and grant our business-need applications permission to run. But that relatively small time investment up front has paid off in huge man-hour savings since going live," said Craig White, one of CMA's Systems Administrators.

"We have been thrilled with how Comodo Advanced Endpoint Protection solution fits into our IT environment. The central dashboard and monitoring allows us to save a tremendous amount of time identifying and containing any possible unknown risk – without threat or interruption to our users," said Clint Davis, IT Manager for CMA. "Before Comodo, we were going through what seemed to be daily malware fixes and problems. Since Comodo, we've had zero malware or spyware issues. We don't fear that unknown, zero day threat because we know the Comodo Advanced Endpoint Protection suite can handle anything the cyber criminals try and throw at it."

Summary

Comodo's Advanced Endpoint Protection solution utilizes a Default Deny Platform to provide complete protection against zero-day threats, without negatively impacting usability for end users. All unknown processes and applications are automatically contained in a secure container, allowing safe applications the freedom to run while denying malware the system access they require to deliver their payloads. Comodo Advanced Endpoint Protection utilizes as little as 10MB of endpoint resources and is hardware agnostic, unlike other competing solutions on the market today. Through the Default Deny platform and consolidation of IT and security management, Comodo solves the malware problem for enterprises large and small.

Get more information on the Comodo Advanced Endpoint Protection solution by contacting

sales@comodo.com

Comodo
1255 Broad Street
Clifton, NJ 07013
United States

About Comodo

The Comodo organization is a global innovator and developer of cybersecurity 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®