Case Study: City of Danville, ILLINOIS

Community Government Will Protect its IT Infrastructure with Comodo Endpoint Security

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

MALWARE IS AN EPIDEMIC

Today, malware threats are everywhere, every day. Anyone who uses computer technology—a smart phone, desktop, laptop, tablet—for business or personal use can be targeted by the “bad guys” of this world. In the last 12 months, dating back to August of 2014, research estimates that more than 350,000,000 pieces of malware have been designed to hack into infrastructures, steal personal information, financial and corporate records, or simply to plant a virus to cause destruction and chaos.

All pieces of malware start out as what can be called unknown files. But with this clear onslaught of millions of pieces of malware each year, the traditional blacklisting of files to keep them away from infecting and breaching the walls of technology infrastructures cannot keep up. Additionally, traditional antivirus solutions focus on detection—not prevention—using default allow technology, which only stops recognized, blacklisted files.

So when that one unknown file does not make it to the blacklist in time, it’s allowed to pass right through into a computer network, and the next cyber-attack happens. All it takes is one employee to open one email attachment that was allowed to pass through because it was not recognized as a bad file.

Scary.

NO INDUSTRY, NO ORGANIZATION IS IMMUNE TO ATTACKS

And what can make this even scarier is that malware isn’t discriminatory. It attacks enterprises large and small. It attacks the infrastructures of banks, hospitals, and non-profit organizations, causing millions of dollars in damages.

For county governments, the risks are the same as large enterprises or the small business: the need to protect and contain their information. The City of Danville, Illinois has a population of approximately 33,000 residents with a small-town feel but big city needs. The City prides itself on its wide range of successful small businesses from antiques and boutiques to big-box stores, large parks, strong academics, and affordable housing.

Like other cities, technology lies at the heart of the City of Danville’s ability to support its residents. The IT department for the City of Danville is tasked in part with keeping safe and protected all the employment records, city finances, business licenses, and public utilities information, while at the same time allowing the City’s endpoint computers to have instant access to share, build, exchange and act upon the information for the benefit of its residents.

"Over the years, we’ve built up an IT infrastructure that relies more and more on the digital file and less on the physical paper file,” said Agnel DSilva, Information Technology Administrator for the City of Danville. “With that move to a more digital environment, it allows us to process information quicker, help our residents faster, and..."
streamline paperwork. But it also increases our risk factor of having sensitive data in cyber space. “We need to keep that information protected and contained at all times.”

TURNING TO COMODO TO CONTAIN AND NEUTRALIZE ANY THREAT

As the rise of malware increases, the City of Danville pulled a proposal together to increase the cyber-security layers it had on its infrastructure and ensure its data was contained. The City of Danville has been using Comodo Digital Certificates for more than a year, and it immediately sought Comodo as the possible technology partner for them.

The City had specific needs in mind: total protection against malware and as much as prevention possible from an attack before it happens, ease of use and installation by a small IT team, while at the same time having little to no impact or intrusion on the IT system’s performance or the users who need to access the information.

After evaluating multiple security companies such as Symantec, FireEye, Webroot and Comodo, the City of Danville chose Comodo and its Endpoint Security Manager as the clear leader to address the City’s needs.

“We selected Comodo and its Endpoint Security Manager solution because it clearly addresses the problem of malware and cyber-attacks through a unique containment technology. Also, its prevention philosophy is different from anything else in the market today,” said DSilva. “Comodo ESM gives our IT team full control over all of our endpoints, allowing for only approved applications to be run, and gives us a remote desktop management and dashboard for simplicity and ease of use, all within our budget.”

As of July 2015, the City of Danville has already installed Comodo Endpoint Security Manager (ESM) on some department computers and servers, with full installation expected by the end of July.

For IT networks who must prevent data breaches such as the City of Danville, Comodo ESM 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 or the user’s productivity.

“As running applications in a contained and protected environment without impacting a single user is phenomenal,” DSilva concluded. “We trust Comodo and its endpoint security solution and look forward to a long relationship.”

Read about the City of Danville, Illinois at http://www.cityofdanville.org/

About Comodo

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 and the Comodo brand are trademarks of the Comodo Group Inc. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. The current list of Comodo trademarks and patents is available at comodo.com/repository

Copyright © 2015 Comodo. All rights reserved.

Comodo
Creating Trust Online®