CaseStudy: Rahr Malting Company

Global Organization Relies on Comodo's Advanced Endpoint Protection Technology to Protect and Secure Its Information

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

Headquartered in Shakopee, Minnesota, the Rahr Malting Company produces and distributes malt and other related brewing supplies to customers around the world. Founded in 1847 by German immigrant William Rahr, the corporation continues to be owned and operated by the Rahr family, now in its sixth generation. Rahr Malting Company has malt production plants located in Shakopee as well as Alix, Alberta, Canada. There is also a barley procurement and distribution center situated in Taft, North Dakota.

Like most organizations today, Rahr Malting Company (http://www.rahr.com/) depends on the online world for the sharing, exchanging and processing of information to keep the Rahr Malting Company in full contact with its employees, customers and business partners.

"As a company that works across a global network, we have hundreds of endpoints in various forms – laptops, desktops and mobile devices – all of which could be at risk for a virus or rogue malware," said Josh Vogel, manager of Network Administration for Rahr Malting Company. "As we expanded and added new employees, we seemed to be expanding our IT risks as well and needed to ensure we had a security solution in place that would protect us from malware and cyberthreats."

HR records, payroll, company policies and procedures are all logged and shared online. Additionally, the company network – which is accessible to those with clearance – holds contracts, confidential agreements and licensing agreements. Rahr Malting Company employees and leadership are continuously using email, Web portals and social media across Ethernet and Wi-Fi hotspots, spanning multiple onsite and offsite locations. All of this key information is utilized and leveraged by the leadership and the full Rahr Malting team across its networks where it can be shared, collaborated on and maximized by the teams.

However, in this age of cybercriminals where social security numbers, financial records and personal and business information needs to be protected and secured – companies and organizations are looking at new cybersecurity alternatives that focus on the prevention of attacks, not just detection when a virus or malware attack has happened.

Fearing the unknown, the zero-day threat has become one of the real-world challenges for the System IT Administrator and IT team at Rahr Malting Company.

Rahr Malting Company'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 – including getting hit with Cryptolocker.

The IT team was encountering rogue malware, Trojans, and viruses across its network and clearing an average of three to five major IT security infections every week. On top of what the IT team was finding, they had to face up to the reality that an unknown rogue piece of malware might be lurking in their network, potentially undetected until it was too late to react.

TURNING TO COMODO FOR ADVANCED ENDPOINT PROTECTION

With various endpoints to contend with, Rahr Malting Company decided to seek out alternative cybersecurity companies that could deliver on their two core needs: manageability of endpoints from a single console and the ability to protect endpoints from infection – both from known and new, unidentified threats.

With these criteria in mind, Rahr Malting Company researched and evaluated Comodo, Symantec, Kaspersky and McAfee. Based on the ability to stop infections cold while providing an easy-to-use dashboard, Comodo and its Advanced Endpoint Protection (AEP) solution were the ideal fit for the company.

Comodo AEP utilizes a Default Deny Platform to provide complete protection for Rahr Malting Company against zero-day threats, while having no impact on any end-user experience or workflows. Any untrusted processes and application are automatically contained in a secure environment, giving safe applications the freedom to run and execute, while denying malware the system access they require to deliver their payloads.

Comodo AEP is also integrated with Comodo's local and cloud-based Specialized Threat Analysis and Protection (STAP) engine, which provides an accelerated verdict of unknown files into either known good or known bad, thus keeping unknown files in containment the shortest time of any solution on the market.

The foundation of Comodo AEP is Comodo Client, which includes antivirus, firewall, Web URL filtering, host intrusion prevention, containment and file reputation; and Comodo IT and Security Manager (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 Rahr Malting Company for panoramic insight and to control all aspects of endpoint protection and management. Its streamlined interface displays critical metrics from all of the endpoints at Rahr, facilitating rapid alerts and quick remediation of issues. Rahr Malting'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.

"We have been thrilled with how Comodo Advanced Endpoint Protection fits into our IT environment," said Vogel. "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 staff."

Comodo Advanced Endpoint Protection brings multiple layers of defense, including antivirus, firewall, Web URL filtering, host intrusion prevention, auto-sandbox (containment), file reputation and virus scope (behavioral analyzer) together under a single offering to protect customers of all sizes from both known and unknown threats. Recently, Comodo unified its endpoint security solutions and enterprise class device management – including Comodo Endpoint Security Manager (ESM) and Comodo Device Manager (CDM) – into Comodo Advanced Endpoint Protection.

Rahr Malting Company has been running Comodo Advanced Endpoint Protection since December 2015 and has not had a single infection.

"Before Comodo, we were going through what seemed to be weekly malware fixes and problems," added Vogel. "Since we brought Comodo in, we've had none of the malware or spyware issues which threaten companies like ours. We don't fear that unknown, zero-day threat because we know Comodo's Advanced Endpoint Protection suite can handle anything the cybercriminals try and throw at it."

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**

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 cyberattack 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
1255 Broad Street
Clifton, NJ 07013
United States