Ovum
TMT intelligence | informa

On the Radar: Comodo protects endpoints by using containment with local and cloud-based inspection

Sale of certificate authority business enables Comodo to focus on product development

Publication Date: 10 Nov 2017 | Product code: INT003-000009

Rik Turner

Summary

Catalyst

Comodo develops security technology for enterprise, small/medium business, and consumer markets. Its enterprise portfolio comprises endpoint, web application firewall (WAF), internet gateway security (the web and email), application containerization, managed security service (MSS), and mobile device management (MDM). The company recently sold a majority stake in its certificate authority (CA) business to private equity to enable it to focus on its product development activity.

Key messages

- Comodo AEP uses whitelists compiled from its SSL certificate business for code that is to be allowed through.
- It uses blacklists of known bad files, file-less malware, and URLs to block certain processes, files, and applications.
- It uses virtualization at the operating system (OS) level to contain untrusted processes while they are inspected locally and in the cloud by machine-learning-based artificial intelligence (AI) and, if needed, by human analysts from its threat lab.
- This combination underpins Comodo's claim that unknown files stay in containment on its platforms for the shortest time of any containment product on the market.

Ovum view

There is a need for technology that can take quick but accurate decisions about whether the untrusted code is good or bad, and AEP clearly seeks to achieve both speed and accuracy. Its use of the web hosting and MSP route makes it appropriate for the SME market and large enterprises that embrace cloud computing.

Recommendations for enterprises

Why put Comodo AEP on your radar?

Comodo AEP is a compelling option for any customer's **endpoint protection** platform (EPP) project. However, Comodo's go-to-market approach of leveraging web hosting and managed service providers (MSPs) will need to be complemented with a more direct one for larger enterprises, and the company clearly still has work to do if it is to break into this segment. Its claim of zero malware infections among customers using AEP is interesting, particularly in light of the containment technology’s minimal impact on productivity.

Highlights

The core capability underpinning AEP is Comodo's Secure Auto-Containment technology, which uses virtualization at the OS level to prevent possible infection while allowing the user to safely access

unknown files. This technique presents a virtual file system, COM interfaces, and registries to the suspect code, which is the "unknown" that is on neither the whitelists nor blacklists of files Comodo identifies via its SSL certificate business (for whitelists) and file and URL lists (for blacklists). This sidesteps any attempt by the suspect to write anything to disk or modify the registries, or to inject malicious code via the COM interface, thereby keeping the suspect contained.

While it is contained, a local AEP component on the device called VirusScope analyzes application behavior and actions running inside or outside of containment, using multiple techniques to determine any malicious intent. Beyond that, a cloud-based component called Valkyrie File Analysis Platform correlates VirusScope's local view of the file's activity with a global view combined with automated and human analysis to reduce false positives and false negatives, providing an accelerated verdict of malware at the endpoint. Comodo claims that unknown files stay in containment on its platforms for the shortest time of any containment product on the market.

By this it means that in 99% of cases, VirusScope alone can reach a decision about whether the suspect code is in fact malicious, and it does this in a very short time. If it cannot, it invokes Valkyrie, in which case additional tools and the human analysts in the Comodo lab look at it and return a verdict within four hours.

Comodo contrasts its OS-level virtualization approach with the isolation technology advocated for security by companies such as Bromium and Menlo Security. Bromium performs the virtualization at the CPU level on the actual endpoint (a desktop or laptop), using an agent on the device that Comodo says is considerably "heavier" (it has a larger footprint) than its own. Menlo, meanwhile, carries out its virtualization in the cloud.

In both cases, isolation continues for as long as a web session is under way, whereas Comodo's approach is to use OS-level virtualization for containment only, releasing what it deems to be the "good", either because it is on the company's whitelist or because it has been found to be innocuous while in containment, into the physical environment of the endpoint.

AEP is underpinned by what Comodo refers to as its Default Deny Platform, which contains all untrusted files and processes so that first VirusScope and then Valkyrie can be invoked. Meanwhile, the speed that these two components enable in decision-making underpins Comodo's claim to offer "Default Deny security with Default Allow usability".

Another component of AEP is its IT and Security Manager (ITSM) management console, which is designed to provide unified cloud-based or on-premise console facilities for security, configuration, and policy management, as well as enterprise visibility.

Background

Comodo was founded in 1998 in the UK by its CEO Melih Abdulhayoglu, and transferred operations to the US in 2004. Its global headquarters are in Clifton, New Jersey, with branch offices in Silicon Valley and 12 across Europe and Asia. The company remains privately held with no VC funding.

Comodo began life as a certificate authority (CA) and launched its first product, Personal Secure Email Certificate, in 2001. It is now the world's largest provider of certificates, with products in some 53% of servers worldwide.

This area of activity had two important benefits. First, it generated the funds to finance the development of its cybersecurity products. Second, it created a network of more than 85 million

endpoints (servers and end-user devices), which Comodo leverages for knowledge of known good files.

In 2005, Comodo diversified into other security product areas and launched a personal firewall product. Its endpoint security technology has been available in the consumer market since 2013, and the enterprise version, the AEP product, launched in February 2016.

In October 2017, Comodo sold a majority stake in Comodo CA to private equity firm Francisco Partners, enabling the product company to focus on establishing a security operations center and further developing its platform.

Current position

A fundamental part of Comodo's go-to-market strategy involves web hosting companies and managed service providers (MSPs) that together amount to some 25,000 partners worldwide.

For this community, it offers a portfolio of free tools for IT management, a platform it calls Comodo ONE, which includes features such as remote monitoring and management (RMM), service desk functionality, remote control and access, and automated patch management. It also embeds an app store in Comodo ONE that includes the enterprise security product for purchase by the partner's customers.

It draws on the network of 85 million endpoints, 95% of which are in the consumer market, for its knowledge of the known good files, while for the known bad files, it uses file- and URL-based blacklists. It then subjects what is not on either list (untrusted processes, files, and applications) to inspection in Valkyrie, which uses a cloud-based sandbox.

The most recent version of AEP was unveiled in February 2017, with OS coverage extended from Windows desktops and servers, Android, and iOS to Mac OSX and Linux.

Data sheet

Key facts

Table 1: Data sheet: Comodo

Product name	Comodo Advanced Endpoint Protection	**Product classification**	Endpoint protection platform (EPP)
Version number	n/a	**Release date**	February 2017
Industries covered	All (horizontal product)	**Geographies covered**	Global
Relevant company sizes	20+ endpoints (for small businesses), scaling to any size large enterprise	**Licensing options**	Subscription-based licensing per endpoint list, with tiered volume discounting available. Comodo AEP includes the Comodo Client, Comodo IT and Security Manager (ITSM), and support (email, phone, and the web) at no extra charge.
URL	www.comodo.com	**Routes to market**	Direct, channels, MSPs
Company headquarters	Clifton, NJ, US	**Number of employees**	1,200

Source: Ovum

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time, they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Further reading

"On the Radar: Comodo offers advanced endpoint protection," IT0022-000667 (April 2016)

Author

Rik Turner, Senior Analyst, Infrastructure Solutions

rik.turner@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum

TMT intelligence | informa

CONTACT US

www.ovum.com

analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

San Francisco

Sao Paulo

Tokyo