Keeping Your Endpoints Free of Malware

Advanced Endpoint Protection

COMODO

Keeping Your Endpoints Free of Malware

Advanced Endpoint Protection

> Gartner estimates that “signature based malware engines are only 30% accurate at detecting new threats.” [1]

Why Traditional Endpoint Solutions Fail

With malware proliferating at an astonishing rate of over one million unknown pieces per day, legacy approaches to endpoint protection have been rendered incapable of defending organizations. Gartner estimates that “signature based malware engines are only 30% accurate at detecting new threats.”[1] The result is that you may be allowing unknown files to run with unfettered access — an open invitation for your endpoints to become infected.

In today’s world of targeted attacks and advanced persistent threats, all it takes is a single infection to cause damage. With Ponemon Institute reporting that the cost incurred for each lost or stolen record containing sensitive and confidential information in 2016 stands a $158 per record with the average consolidated total cost hitting $4 million,[2] organizations cannot afford to be breached.

Why New Approaches Still Fail

To address the inadequacy of traditional signature-based solutions, new endpoint security approaches have been developed that seek to expedite the identification of unknown malware and zero-day exploits. These include automated behavioral analysis tools such as “sandboxes” that run unknown files in virtualized environments, in an effort to see if applications exhibit malicious behavior or not. While this has improved detection rates, it decreases usability as the end user must wait for the analysis to complete before being able to use the file. More concerning, these models take time to “study” these unknown files, a delay that opens a window for malicious files to infect the endpoint. Unfortunately, that single “patient zero” infection is all an attacker needs to pivot and gain access to sensitive assets in your network. These new approaches result in a **Default Allow** security posture, a posture that by default allows everything onto the endpoint unless it’s known to be bad. It’s not the bad files we know about that are the issue, it’s the unknown files that end up being malicious that cause the damage.

COMODO

[1] Gartner Research Inc., TRUE Default Deny and the end of Patient Zero
[2] 2016 Ponemon Institute Cost of a Data Breach Study: https://securityintelligence.com/media/2016-cost-data-breach-study/

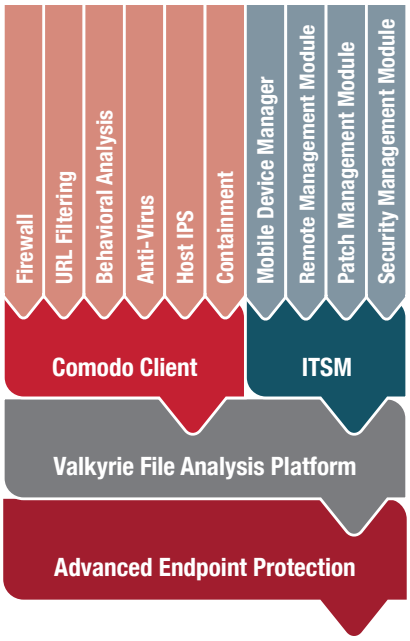
Improving Your Posture

Since the **Default Allow** posture is the underlying problem, we need to flip an organization's overall security posture to Default Deny to eliminate malware threats. Comodo® Advanced Endpoint Protection solution provides a true **Default Deny** security posture enabling complete protection against zero-day threats. But, doesn't a default deny posture bring extreme usability issues?

Not the way we do it. Comodo Advanced Endpoint Solution changes your security posture from Default Allow to Default Deny, while having no impact on the end-user experience or workflows because users can engage unknown files safely while they are in the virtual container.

Let's explain: Comodo AEP provides a multi-layered endpoint defense that **allows** unfettered access to all known good files, **denies** access to any known malicious files, leaving only the **unknown** files to contend with.

This is where Comodo AEP changes everything — Comodo Advanced Endpoint protection allows the user to run those unknown files on the endpoint but they are automatically wrapped in a self-contained file system. This "container" allows the user to run and interact with these files but protects critical endpoint resources from harm. While an unknown file is contained, Comodo AEP is using local and cloud-based file analysis tools and resources to determine its true character. The process is transparent to the end users. If the file is good, it goes on the white list and if it's bad it's eliminated. Comodo AEP's automatic containment functionality is extremely lightweight, has no CPU dependencies and is completely application agnostic.



Accelerated File Analysis

VirusScope™ the behavioral analyzer component of Comodo Security Client, provides local file analysis using behavioral techniques and heuristics to analyze contained unknown files, providing analysis even while the endpoint is disconnected from the Internet. The VirusScope behavior can be tailored to meet the specific needs of an organization, from analyzing all files to only unknown files. While local analysis is taking place, Comodo AEP simultaneously takes file analysis to the cloud — Valkyrie, Comodo's cloud-based file analysis tool, correlates the VirusScope local view of the file's activity with a global view. This avoids false positives and false negatives and provides an accelerated verdict to identify malware at the endpoint. The result is that unknown files stay in containment for the shortest time of any containment solution on the market.

Valkyrie combines static, dynamic and human expert analysis with machine learning techniques to deliver a verdict on over 95% of the unknown files it sees in less than 45 seconds. Files needing more in-depth analysis will undergo human analysis by security experts within Comodo's Threat Research Labs (CTRL).

Comodo Client Security

Comodo Client Security is the portion of Comodo AEP that runs directly on the endpoint, delivering a layered suite of protection that is both lightweight and scalable. Comodo Security Client integrates:

- **Automatic Unknown File Containment**
- **Personal Firewall**
- **File Lookup Service**
- **Host Intrusion Prevention (HIPS)**
- **File-less Malware Prevention**
- **Antivirus**
- **Web Filtering**
- **Behavioral Analysis (VirusScope)**
- **Integration with Valkyrie Cloud-based Static, Dynamic and Human Expert Analysis**

All of this functionality is delivered in a lightweight, integrated client security solution that provides your endpoints with a true Default Deny security posture, centralized management and a great user experience.

More Than Malware Prevention

Comodo Advanced Endpoint Protection solution delivers a **Default Deny** Platform, leveraging automated file containment technology that allows unknown files to run in a safe, contained environment while analysis determines a file's true state. In addition to preventing known and unknown malware from executing, a complete endpoint protection solution also must include the administration of security patches, OS updates and application visibility and control, along with **remote administration and management** of external devices. In the past, organizations have had to deploy multiple solutions to accomplish these tasks. Today, Comodo has integrated these critical IT and security management components with cloud-accessible Advanced Endpoint Protection under a single, unified platform.

Integrated with Comodo AEP is Comodo's IT and Security Manager (ITSM) that delivers management tools for security policy management and deep visibility into the security posture and health of your enterprise endpoints. ITSM mobile device and inventory management capabilities allow for the remote provisioning, configuration and control of Android, iOS and Windows-based devices — from a single pane of glass. This includes tasks such as restricting what a user can do on corporate-owned mobile devices, remotely wiping devices, locking down USB ports and identifying the geographic location of a device. Part of the Comodo AEP solution, **ITSM** delivers complete centralized management and control over all of your organization's endpoints.

Application Visibility & Control	Easy Onboarding	Product Development & Malware Research Teams
– Provides administrators with enterprise wide visibility and control over what applications users are installing across Windows-enabled endpoints with device management capabilities – Windows applications can be permitted, blocked or allowed to run only inside a secure container – Increase productivity by blocking non-critical business applications from running – Ability to set mobile application policies, based on groups (productivity apps, utility apps, gaming apps, etc.) – Provides another layer of endpoint protection and management	– Makes tedious provisioning easier – Integrated Auto Discovery provides an easy tool that finds and inventories the endpoints in your organization from laptops to mobile and even BYOD devices – After inventory creation, automatic deployment and over-the-air provisioning makes it easy to bring those devices under central control and management	– World's largest certificate authority brand – Uniquely positioned to identify known good software publishers and applications (whitelists) – Installed base of over 85 million Windows antivirus users provides the Comodo Threat Research Lab (CTRL) with one of the largest caches of known bad files (blacklists) – Global product development and malware research team has security professionals working 24x7x365 worldwide to ensure that unknown files are rapidly identified before they are able to cause damage

Comodo Advanced Endpoint Protection

Advanced Endpoint Protection combines the functionality of the best in endpoint protection and cloud-based file analysis, with complete IT and security management. Comodo AEP gives you the power to manage devices and stop malware and breaches from affecting your organization with a true Default Deny security platform. You can protect your endpoints from both known and unknown malware while delivering a great user experience.

About Comodo

The Comodo organization is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Building on its unique position as the world's largest certificate authority, Comodo authenticates, validates and secures networks and infrastructures from individuals, to mid-sized companies, to the world's largest enterprises. Comodo provides complete end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats, both known and unknown. With global headquarters in New Jersey and branch offices in Silicon Valley, Comodo has 12 international offices across Europe and Asia.

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

Comodo Group, Inc.
1255 Broad Street
Clifton, NJ 07013
United States

Tel: +1 (888) 266-6361
Tel: +1 (703) 581-6361
Fax: +1 (973) 777-4394

sales@comodo.com
enterprise.comodo.com

COMODO

AEPSB120116a