COMODO

Science meets Cybersecurity

ALAN TURING, UNDECIDABLE PROBLEMS AND MALWARE

Enterprises move fast along with the expanding attack surface. This means there will be untrusted applications that any legacy or automated detection method cannot identify reliably within a reasonable time. This undecidable problem (e.g. Halting Problem), proven by Alan Turing in 1936, translates into scientific proof that your security solution will fail to detect some of the malware.

No one can stop zero-day malware from entering your network, but Comodo can prevent it from causing any damage.

Zero infection.

Zero damage.

WHAT WE DO

Comodo solves the most advanced malware problems with innovative solutions that secure the enterprise from both known and unknown threats across the endpoint, boundary and internal network.

COMODO

Science meets Cybersecurity

COMPANY FACT SHEET

FAST FACTS

INDUSTRY
Computer and Internet Security

FOUNDED
1998 United Kingdom

HEADQUARTERS
US – Clifton, New Jersey
Offices – APAC, EMEA

PRESIDENT, CEO and FOUNDER
Melih Abdulhayoğlu

NUMBER OF EMPLOYEES
1,000+ Over half are engineers

CUSTOMERS / PARTNERS
- *20% of the Fortune 1000*
- *800K business customers in 100 countries*
- *20K business partners and affiliates*
- *100 million + PC security installations*

PRIVATELY HELD
Profitable

PATENTS / Patents Pending
250+

INDUSTRY LEADERSHIP
2017 – World's Largest Certificate Authority: 53.6% global market share

2005 – Founder, CA/Browser Forum: promotes Internet security standards and baseline requirements

ENTERPRISE CYBERSECURITY

Comodo Advanced Endpoint Protection

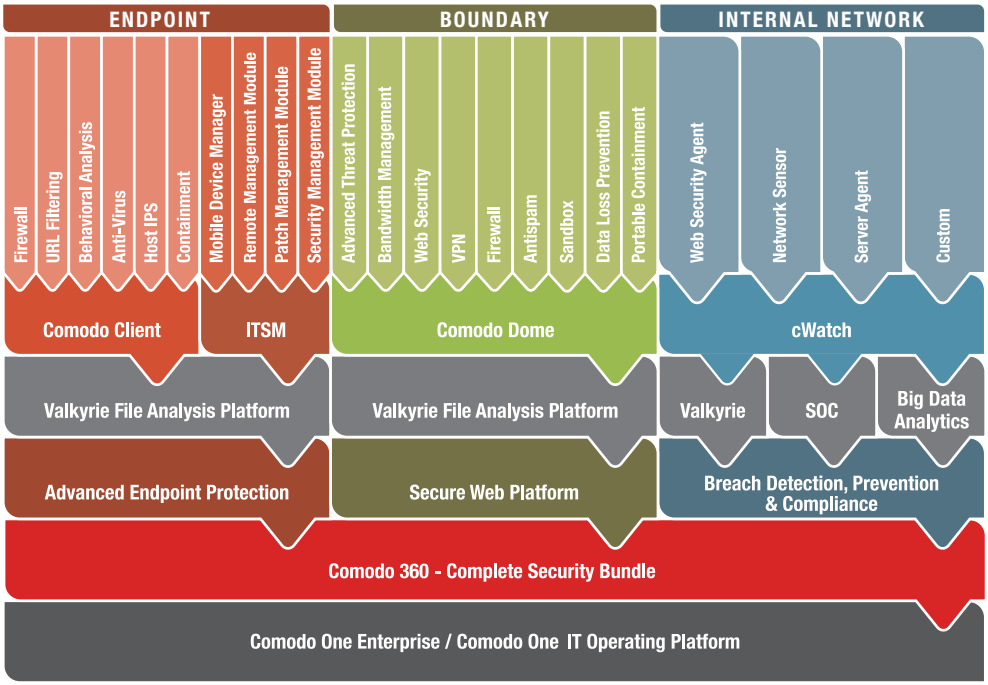
Why are data breaches on the rise? Enterprises keep getting infected because conventional endpoint protection solutions—including next-generation automated approaches—detect only the files and applications that are known to be bad. They allow everything else to run on the endpoint and this Default Allow posture is how zero-day threats get into your network. All hackers have to do is create new malware to avoid detection. Allowing only one percent of untrusted applications or processes to run in your enterprise invites attack.

Comodo is the only security vendor with a Default Deny platform that allows full usability of unknown files while they run in Secure Auto Containment™ until automatic and expert human analysis delivers a trust verdict of good or bad. Comodo Advanced Endpoint Protection is based on a Default Deny posture that allows the good applications, blocks the bad, and contains the unknown files pending analysis to prevent the damage from unknown malware. Only good files run unfettered on your endpoints.

Comodo's Secure Auto Containment technology is extremely lightweight, has no CPU dependencies and is completely application agnostic. This gives enterprises and end users the best of both worlds: default deny security with default allow usability.

Operational Efficiency with Adaptive Enterprise Security Platform

Comodo's integrated solutions at the endpoint, boundary and internal network exchange threat intelligence and other information across the enterprise to prevent the damage from cyber-attacks. This helps enterprises lower costs while addressing their complete cybersecurity needs with greater operational efficiency.



COMODO

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
www.enterprise.comodo.com