Email Problem Solved

Comodo Email Security

COMODO

Comodo Email Security

Only Comodo combines antispam with the total security of a Default Deny Platform and the flexibility and operational freedom of default-allow. This game changing innovation solves the email security problem.

Spam Filtering for the Cloud Era

Comodo Email Security manages and filters all inbound and outbound email traffic to provide complete protection for your organization from the ever-increasing deluge of spam, sophisticated email-borne threats and sensitive data leaks. Next generation pre-perimeter spam, phishing, and malware protection ensures clean emails are delivered safely while unwanted email content is blocked by an advanced combination of over 20 layers of deep content inspection, as well as Comodo Threat Research Labs analysis and a server reputation network that can flawlessly identify human vs machine based email senders. This ensures each incoming email poses ZERO risk to your end users.

As a complete email management solution, Comodo Email Security can be either 100% SaaS delivered, deployed on-premises, or on your choice of cloud platforms.

Advanced Office 365 Protection

Migrating your email services to a cloud based service like Microsoft Office 365 gives your organization reduced management overhead and versatile access to email. However, trusting your critical data to the cloud raises important security, compliance and data protection concerns. Comodo Antispam Gateway (ASG) provides revolutionary multi-layer security, archiving and backup, allowing you to operate faster, safer and more efficiently in Microsoft Office365 and other cloud platforms.

"There is so much malware and spam in the world today...Comodo technology contains all threats – known and unknown – and keeps my IT environment secure."

~ Enterprise Customer

COMODO

Solution

Comodo's email security solutions provide advanced platforms that completely protect your network from spam, phishing, and ransomware while at the same time restoring capacity currently lost to unwanted spam traffic and reducing mail server processing load—up to 70 percent or more.

A full set of advanced features allow you to centrally administer policies and permissions at an individual or group-based level while flexible deployment options allow you to choose between a fully hosted solution in Comodo Antispam Gateway (ASG) or to deploy as a virtual appliance with Comodo Korumail.

Each of the Comodo Email Security Solutions provides industry leading protection from even the most sophisticated malicious file attachments by leveraging two key Comodo Threat and Research Labs technologies:
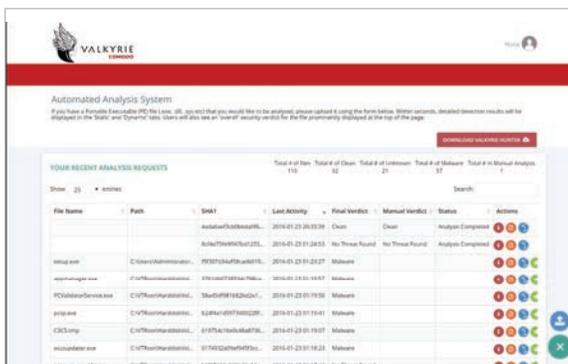
Valkyrie Cloud-based File Verdicting

Valkyrie leverages static detection, dynamic and behavioral analysis, advanced heuristics and expert hands-on human inspection to analyze files and URLs found in incoming and outgoing emails. It quickly renders a verdict of unknown, known-bad (blocked) or known-good (passed). Unknown files are placed in containment and passed on for delivery to the user while undergoing more extensive analysis, including examination by human experts. When a final verdict arrives—normally within seconds—the file is released from containment or deleted and blocked.

Comodo Advanced Containment

Sandboxing is becoming a commonplace security strategy, but it typically hinders business productivity by isolating unknown and suspect files in a state where they cannot be used until after analysis. Comodo's unique containerization technology is different. While Valkyrie analyzes unknown files, email recipients are free to open, execute and use the files without any risk of infection. Comodo's containment technology is extremely lightweight, has no CPU dependencies and is application-agnostic. It ensures you have both the complete security of a default-deny platform and the operational freedom and productivity of default-allow.
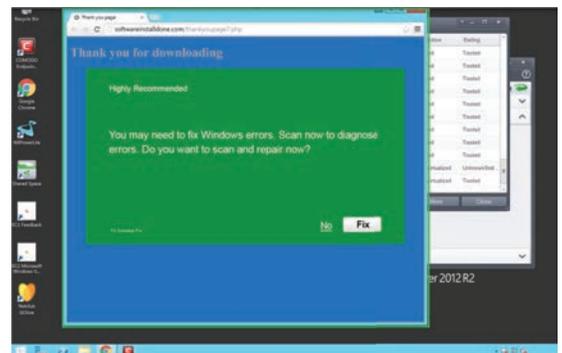
Comodo's Default Deny Platform places an emphasis on allowing known good applications, while denying everything else until a verdict is reached. In order to execute on this strategy, identifying known good and known bad applications is critical. As the #1 largest certificate authority brand in the world, Comodo is uniquely positioned to identify known good software publishers, applications (whitelists); while our installed base of over 85 million users provides the Comodo Threat Research Lab (CTRL) with one of the largest caches of known bad files (blacklists).

COMODO

Email Security Problem: Solved.

Traditional email security is built on a default-allow design combined with block lists and signature-based detection, but with new malware variants at a million per day and climbing, a solution that relies on "patient-zero" infections for detection guarantees you'll be infected eventually. This is the basic problem of email security today and it is clear that current solutions are not adequate to protect your organization in an environment where 70% of email received is unsolicited, and almost 80% of corporate malware infections originate from phishing emails and infected attachments.

Enterprise-ready Capabilities

Fully protect cloud based (Office365), as well as on-premises email servers	Comprehensive email archiving and logging for Auditing, forensic analysis, compliance, discovery and arbitration
Ensure 100% protection from malicious file attachments and email based threats	Rapid deployment with Active Directory/LDAP integration and automated e-discovery of recipients and senders
Reduce administrative overhead with centralized, granular, group- and user-based email policy management	Control data loss by defining which file types are allowed to enter or leave the organization

Comodo solves the email security problem with advanced antispam capabilities in conjunction with a revolutionary Default Deny architecture that takes full advantage of Comodo's Valkyrie cloud file verdicting system to rapidly identify all known good, known bad and, most importantly, unknown attachments before they are delivered to user mailboxes. Even if a file is classified as unknown and unrecognized by all antivirus engines on the market, Comodo's advanced portable containment technology allows users to receive, access and execute attachments, with zero chance of infection.

Reclaim your email with a range of cutting-edge technologies that will enable your organization to archive and respond to emergency situations, while at the same time effectively detect and block spam, malicious emails, and targeted attacks.

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 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 comodo.com.