COMODO

Comodo Secure Email Gateway

At-a-glance

- Enterprise-class antispam with flexible deployment options: dedicated hosted cloud and on-premises for enterprises and multitenant cloud for MSPs.
- The perfect balance of security and usability through patent-pending threat containment and analysis
- Unmatched visibility into threat activity worldwide via intelligence gathered from over 86 million endpoints under Comodo Cybersecurity's management
- 400 million messages filtered last year—340 million pieces of spam caught and 4 million malicious emails blocked

Blocking Spam and Malicious Emails to Bolster Productivity and Security

Spam is more than an annoyance; it is a costly productivity-killer and time-waster. Large volumes of unwanted email burden systems and users alike. What's worse is that amid all of the spam flowing into the corporate network are emails sent with a single purpose: to deliver a malicious file. Comodo Cybersecurity offers Comodo Antispam as a 100% cloud-delivered service with both singletenant and multi-tenant management options. Comodo Antispam protects businesses from the daily onslaught of spam and malicious emails—without any IT footprint or security staff.

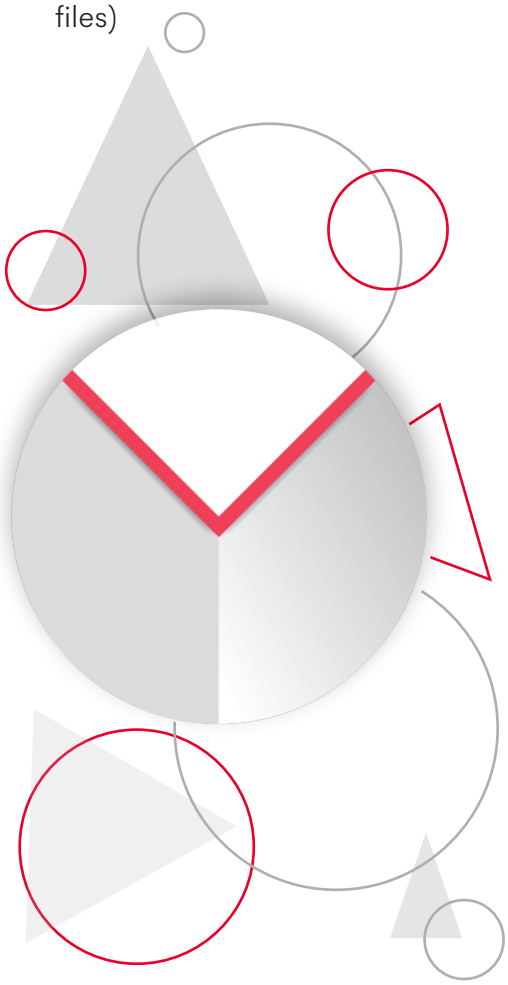
Balancing Security and Usability

Given the pace at which cyberthreats evolve, it is simply not possible to detect and stop every threat that enters the network before it does its damage. In the time it takes to recognize and respond to a novel threat, critical systems and information can be compromised. Comodo Cybersecurity assumes all unknown files to be risky until proven otherwise. We wrap all unknown files in a container, placing them in an isolated environment while they undergo a security analysis. This containment enables business users to continue working with a file in parallel to its analysis—thus security does not hinder the business.

COMODO

Valkyrie

Valkyrie—Comodo Cybersecurity's threat analysis engine—is the only platform in the world to deliver a 100% trusted verdict on all unknown files, classifying them as known good or known bad. Valkyrie Verdict provides real time visibility into what's happening across your whole network by leaving no files unchecked. 100% of all files that are not classified are analyzed at lightning speed, then moved to either a known good and known bad state. No other endpoint vendor provides 100% visibility into the customer's network (as the assumption-based verdicting doesn't know about undetected files)



Features

Comodo Antispam offers a comprehensive set of features:

SECURITY FEATURES

- Antivirus scanning (Comodo Antivirus and Comodo Valkyrie integration)
- Automated unknown file portable containment (sandboxing)
- Spam filtering
- Phishing protection
- Real-time spam and malware signatures
- Denial of Service (DoS) protection
- Domain key antispoofing technology (DKIM)
- SMTP IPS/firewall

SPAM FILTER

- Integrated with Comodo Antispam Labs
- Sender Reputation Network (RN)
- Server behavioral analysis
- RBL and DNSBL support
- Reverse DNS intelligence
- Machine vs human intent identification
- Spam database pattern matching
- IP reputation analysis
- Bayesian analysis
- Fingerprint analysis
- Image spam identification
- Rate controls
- URL fingerprinting
- Anti-fraud protection
- Spam training
- Intelligently learns and adapts to new spam techniques
- Banner and plug-in filter
- Outgoing email filtering
- Sender/recipient filtering
- Auto email classification

MALWARE FILTER

- Comodo Threat Research Labs
- Automated containment
- Static, dynamic and human analysis
- Decompression of archived attachments
- File-type blocking
- Real-time signature updatess

ADVANCED POLICY CONTROLS

- Set independent policies for incoming and outgoing emails
- Per-domain configuration and control
- IP and content-based filtering
- Keyword blocking
- Regional blocking
- TLS encryption policy
- Sent email limitation based on user name and domain

EMAIL CONTINUITY

- Failover to alternate destination
- Web access to spooled email during outage
- Archiving and backup
- High availabilit

USER FEATURES

- Web-based email access
- Per-user blacklist/whitelist
- Per-user quarantine
- eDiscovery of email users

SYSTEM FEATURES

- Easy web-based management interface
- User authentication (LDAP, Active Directory, MySQL, LocalDB)
- Office 365 support
- Delegated domains
- Forensic-grade auditing of all management events
- Automatic whitelisting
- Per-domain settings and control
- Comprehensive scheduled reporting and alerting
- Instant control of quarantined emails through management interface
- Ability to set email attachment size limits

DATA LEAK PREVENTION

- Prevent data theft via emails
- Search for configured words in incoming and outgoing mails
- Apply actions through profile settings – quarantine the mail and/or notify the administrator

COMODO

Here are some frequently asked questions and answers about Secure Email Gateway. Let us know if you can't find the answer you are looking for!

Q: How does Secure Email Gateway protect against email threats?

A: Secure Email Gateway uses a multilayered approach to provide the most comprehensive email protection available against spam, viruses, spoofing, phishing and spyware attacks. Because Secure Email Gateway optimizes email processing, it can filter millions of messages per day. Industry-leading features of Secure Email Gateway are predictive sender-profiling and real-time protection. In addition, Secure Email Gateway includes many explicit defense layers, such as denial of service and security protection rate controls, IP reputation analysis, sender authentication, recipient verification, virus protection, policy (user-specified rules), fingerprint analysis, intent analysis, image analysis, Bayesian analysis, and a spam rules scoring engine.

Q: How is email filtered?

A: Since Secure Email Gateway is deployed at the network perimeter, all incoming email must pass through all defense layers of Secure Email Gateway before any of it can reach the intended recipients. The defense layers are grouped into two main classes: connection management, which involves dropping incoming mail connections before their receipt, and mail scanning, which analyzes messages upon receipt. During the filtering process, emails are checked for new and familiar spammer attacks, viruses, and customized administrator policy violations. Based on administrator and user preferences, spam can be tagged, quarantined or blocked.

Q: By default, what happens to a spam-detected message?

A: The majority of spam is rejected through connection filtering, which is based on the IP address of the sender. Comodo Antispam then inspects the contents of remaining messages to determine if they are spam based on their content. By default, content-filtered spam is sent to the recipients' inbox with a [SPAM] tag, but you can change this action. For example, you can choose to send spam messages to the quarantine instead by configuring the spam filter policy.

Q: What's a zero-day spam variant and how is it handled by the Secure Email Gateway service?

A: A zero-day spam variant is a first generation, previously unknown variant of spam that's never been captured or analyzed, so our spam content filters don't yet have any information available for detecting it. After a zero-day spam sample is captured and analyzed by our spam analysts, if it meets the spam classification criteria, our spam content filters are updated to detect it, and it's no longer considered zero-day.

COMODO

Q: Can Secure Email Gateway limit inbound messages?

A: Yes. Secure Email Gateway lets you set limits for incoming emails for both users and domain names. You can also configure it to allow only a certain number of incoming emails per hour and per day.

Q: What are the underlying technologies used in Secure Email Gateway?

A: Secure Email Gateway uses a combination of proprietary and open source software. The Secure Email Gateway operating system is based on a hardened, stable Linux kernel that has undergone strict scrutiny by top security researchers. Secure Email Gateway is constantly updated in real time by the Comodo Antispam Laboratory. In addition, Secure Email Gateway includes, and is integrated with the Comodo Valkyrie file verdicting engine (https://valkyrie.comodo.com).

Q: How does Secure Email Gateway protect against “dictionary” attacks?

A: Secure Email Gateway includes a user verification feature that uses Lightweight Directory Access Protocol (LDAP) to verify recipients before delivering messages to the email exchange server.

Q: What new technologies has Secure Email Gateway added recently to combat the latest threats?

A: Secure Email Gateway includes numerous advanced techniques to combat the newest cybersecurity threats. For example, it provides auto whitelisting, AI (artificial intelligence) whitelisting and greylisting. In addition, Secure Email Gateway Platinum includes integration with Comodo Containment Technology and the Comodo Valkyrie file verdicting engine (https://valkyrie.comodo.com).

Q: How does Containment work?

A: Containment protects users from zero-day malware by opening any untrusted attachments in a secure, virtual environment. This environment is known as the container. Items in the container are not allowed to access other processes or user data and will write to a virtual hard drive and registry. This isolation means the attachment cannot damage the host machine nor steal confidential information.

Q: How does auto-whitelisting work?

A: Auto-whitelisting, based on artificial intelligence, allows administrators to automatically whitelist sender addresses of incoming and outgoing mails. Auto-whitelisting automatically determines whether traffic between specific email addresses is safe based on predefined thresholds and decides whether or not the sender should be whitelisted.

COMODO

Q: What does greylisting do?

A: Greylisting is another form of spam control in which Secure Email Gateway temporarily rejects email from senders it does not recognize. Instead, it will send a "try again later" message to the sending email server. Upon receiving this message, legitimate email servers will try to resend the email after a delay. Secure Email Gateway will accept the re-sent email only if it is not rejected by other filters. Because of the prohibitive cost of resending millions of emails, spam servers are unlikely to perform this simple resend. This means greylisting can be very effective at blocking large amounts of spam at its source.

Q: How does Secure Email Gateway protect against virus threats?

A: Secure Email Gateway provides comprehensive protection against virus threats through three powerful layers. The first layer consists of virus-scanning engines. The second layer is a proprietary virus engine maintained by the Comodo Antispam Laboratory, an advanced security operations center that works to continuously monitor and block the latest Internet threats. The third layer is Comodo Containment Technology, a set of advanced technologies that enables Secure Email Gateway to immediately block the latest virus, spyware and other malware attacks as they emerge.

Q: How does Secure Email Gateway block real-time threats?

A: Comodo Antispam Laboratory engineers diligently and continuously monitor spam and virus threats around the world. Since response time is critical with zero-day threats, when one is detected, Secure Email Gateway protects you in real-time to mitigate these threats as they emerge without waiting for new Secure Email Gateway update packages.

Q: What is the pricing for Secure Email Gateway?

A: Pricing will vary based on your needs, but there are two types of pricing packages. The Secure Email Gateway Platinum package is licensed based on only the number of users. The Secure Email Gateway Gold package is licensed based on the number of users, the number of domains, and optionally, backup space requirements.

Q: Does Secure Email Gateway offer per-user policies?

A: Per-user policy settings are available in Secure Email Gateway. Per-user policies empower users to set their own individual scoring policies, Bayesian databases, allow lists and block lists.

COMODO

Q: Can Secure Email Gateway filter outbound messages?

A: Yes. Secure Email Gateway filters outbound messages for viruses and spam scanning policies according to predefined settings.

Q: Does Secure Email Gateway block email from other countries?

A: Yes, Secure Email Gateway offers administrators several different ways to block spam from other countries. Administrators can

- Configure geolocation-based restrictions or permissions
- Specify blocking of messages whose top-level domain resolves to a particular country's hostname
- Block messages that contain a specific language set based on the declared character set of an email
- Create custom policies to filter other patterns in the email subject, header or body

Q: How do I know which Secure Email Gateway package is best suited to my needs?

A: Your Comodo sales representative can evaluate your environment based on the number of active users, domains, email traffic and desired features. As your organization expands, your Secure Email Gateway package can be enlarged in order to accommodate your growth.

Q: How does Secure Email Gateway protect organizations from spear-phishing and BusinessEmail Compromise (BEC)?

A: Spear-phishing attacks are highly personalized and typically very low volume with no malicious attachments or links inside. Because of this, they are very hard to stop with existing email security solutions. Secure Email Gateway includes a comprehensive artificial intelligence (AI) solution for real-time spear-phishing and cyberfraud defense. Delivered as a cloud service, Secure Email Gateway combines a powerful AI engine, domain fraud visibility using DKIM (DomainKeys Identified Mail) and anti-fraud training into a comprehensive solution that protects people, businesses, and company brands from spear-phishing and business email compromise (BEC) as well as impersonation attempts and cyberfraud.

COMODO

About Comodo

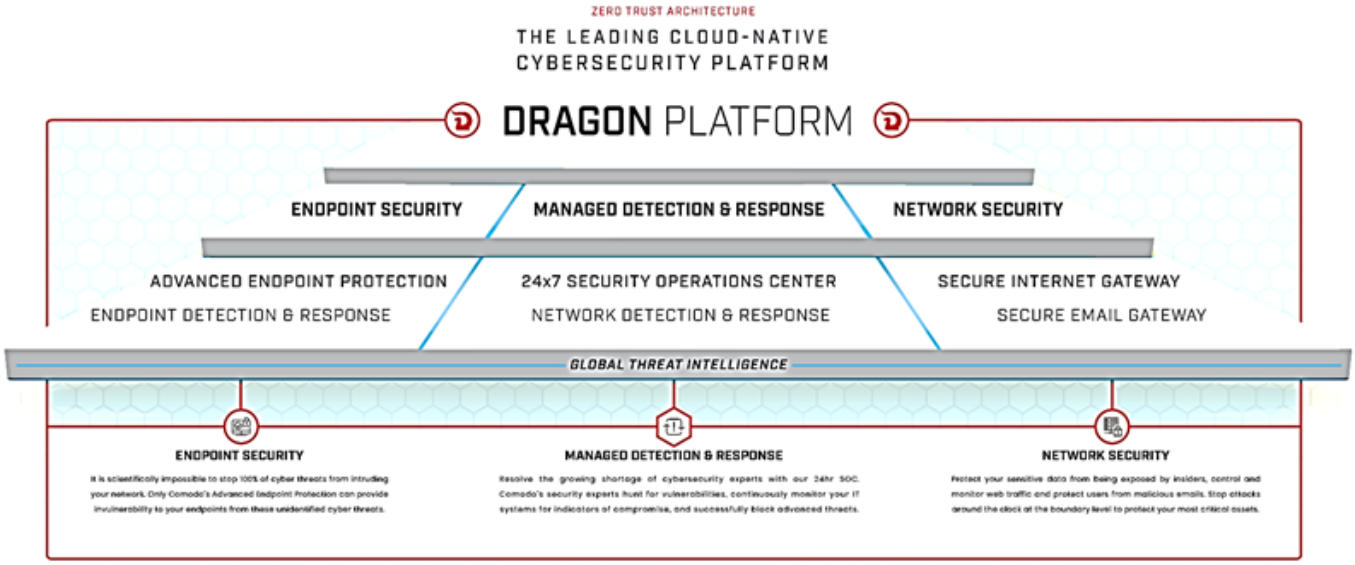
In a world where preventing all cyber-attacks is impossible, Comodo provides active breach protection with its cloud delivered, Zero Trust platform. The Comodo Dragon platform provides a Zero Trust security environment that verdicts 100 percent of unknown files. The platform renders an almost immediate verdict on the status of any unknown files, so it can be handled accordingly by software or human analysts. This shift from reactive to proactive is what makes Comodo unique and gives them the capacity to protect your business—from network to the web to cloud—with confidence and efficacy.

Comodo has experts and analysts in 185 countries, protecting 100 million endpoints and serving 200,000 customers globally. Based in Bloomfield, N.J., Comodo has a 20-year history of protecting the most sensitive data for businesses and consumers worldwide.

ACTIVE BREACH PROTECTION FOR YOUR BUSINESS

Comodo provides Active Breach Protection in a single platform. No one can stop 100% of threats from entering their network so Comodo takes a different approach to prevent breaches.

Experienced intrusion? Contact us at 1 (888) 551-1531
Visit comodo.com for your free 30-day trial



200 Broadacres Dr,
Bloomfield, NJ 07003

Tel: +1 (888) 551-1531
Tel: +1 (973) 859-4000

www.comodo.com
platform.comodo.com