MyCyberIQ™
STAY AWARE. STAY SMART. STAY SECURE.™

Security for Email

Multi-layered, cloud-based email security for your entire organization

Security for Email provides businesses comprehensive email security and protection from known and emerging threats, including impersonation attacks, Business Email Compromise (BEC), CEO fraud, phishing, ransomware and more. Advanced threat intelligence combines traditional pattern message attributes and characteristic matching with algorithmic analysis to deliver the ultimate threat detection and protect networks against targeted email attacks - with almost no false positives.

Security for Email is both an advanced email security solution and a full cloud-based email routing engine with fully featured company and personal quarantines for message management. Deep categorization – distinguishing between professional marketing and suspected mass email campaign messages, for example – enables flexible policies that detail precisely how different types of messages are processed and tagged.

Key capabilities

- **Multiple signature and behaviour-based antivirus engines –** protect against all forms of malware, including zero-day variants

- **Invaluable, detailed message tracking for email admins –** allowing quick view to determine exactly why an email was delivered or rejected, including email headers and the full conversation with the remote email server

- **Multi-layered protection from threats –** multiple security engines use a combination of advanced technologies to detect spam and more sophisticated, targeted phishing and impersonation attacks

- **Traditional pattern, message attribute and characteristic matching –** complemented by algorithmic analysis for ultimate threat detection without impacting accuracy

- **Complete control over email flow with a powerful policy engine enables control over email delivery and message filtering based on attributes such as size, source, destination, keywords and more**

- **User protection in real time –** time-of-click protection rewrites links in messages and protects employees in real-time by blocking and warning users of malicious links

- Outbound filtering helps control content in outgoing messages to prevent IP blacklisting

- **Deep analysis & inspection –** a deep analysis by the multi-scanning engines inspects all aspects of emails, including their size, content, attachments,

At-a-Glance

Our email security solution is 100% cloud-based and easy to deploy. Our policy engine uses multiple AV engines, including static sandboxing of file attachments, and offers a full analysis of inbound and outbound email analysis using unlimited keyword lists. It also protects all email service providers and supports hybrid environments using Exchange on-premise, Microsoft365, Exchange Online, or Gmail.

Key Benefits

- **Advanced behavioral analysis –** leverages advanced analysis, which includes more than 10,000 algorithms analyzing more than 130 variables extracted from each email message, for strong threat detection and prevention.

- **Management and control –** IT administrators have full control to customize how mail flows in and out of the organization, create unlimited keyword lists, and use rules to analyze messages and act based on confidential or sensitive information.

- **Fortified email security –** multiple scanning engines and technologies ensure enterprise-class threat detection that's easy for businesses of any size to implement and manage.

"I'm all about streamlining, simplifying, and making things consistent across the board. So, MyCyberIQ was a great opportunity to consolidate and manage our endpoint and email security across our physical and Azure cloud environments from one console."

Andrew Black, CIO
A-Core Concrete Specialists

headers, sender, recipients and links, then automatically takes actions such as deliver, quarantine, re-route, notify or reject the email

• **Fraud blocking –** blocks non-malware threats such as credential phishing, BEC attacks, CEO fraud and more.

• **Full control –** provides complete control over mail flow, supports multiple email providers and seamlessly integrates with Microsoft 365

A sophisticated policy engine allows the IT administrator to customize exactly how email flows in and out of the organization. The engine can inspect all aspects of email, including size, content, attachments, headers, sender and recipients, and take appropriate actions, such as deliver, quarantine, company quarantine, re-route, notify or reject.

Multi-layer scanning

Multiple traditional signature- and behavior-based AV and anti-spam engines can detect all forms of malware and spam, including zero-day variants. Security for Email has a 99.999% spam detection rate – with near zero false positives and 100% virus protection.

QUARANTINE

EMAIL

Inbound email redirected through GravityZone Email Security cloud servers by changing MX record.

Outbound email redirected via smarthost

Email traffic

Rejected (SMTP error)

CONNECTION FILTERING

MESSAGE FILTERING

Antimalware, Antispam, Antispoofing (SPF, CEO Fraud), Threat Intelligence, Marketing Email Detection, URL rewriting, Custom rules

CLEAN EMAIL

SMTP MAIL SERVER (OFFICE 365)

Clean email delivered to customer server

EMAIL SECURITY CONSOLE POLICY MANAGEMENT & REPORTING