CORVID

CORVID EMAIL PROTECTION

Comprehensive email security that stands between your users and adversaries.

Email is an essential communication platform for businesses and individuals alike, but it's also the biggest attack vector. It allows cyber attackers to contact users directly, where ordinary defensive barriers can't protect them. With traditional attack methods (such as malware attachments) being blocked at the boundary, email-based attacks are increasing in complexity and sophistication – attackers are turning to more subtle means to trick users into undertaking activity that results in a compromise. Techniques such as adjacent letter transposition and Punycode letter substitution defy detection by even the most diligent of users.

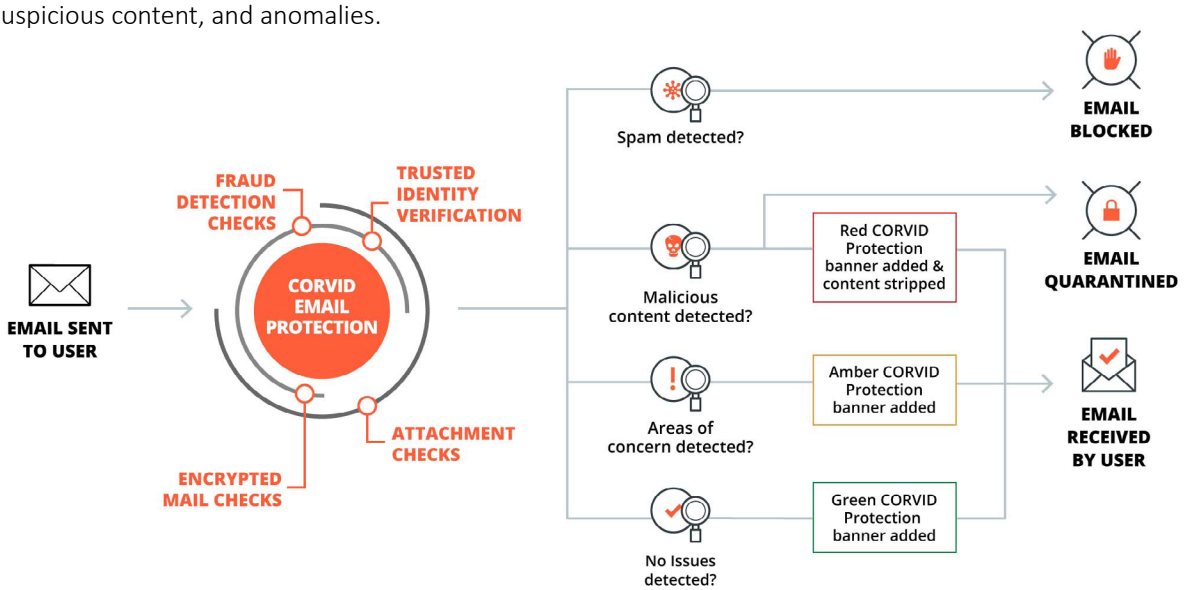
What is CORVID Email Protection?

CORVID Email Protection scans all inbound emails so users don't need to be trained in attacker techniques and trends.

- Stops malicious emails before they get to your inbox.
- Displays a warning if an adversary is attempting to mislead, harvest credentials, or spread malware.
- Provides an intuitive guard against fraud, impersonation, and spam attacks.
- Gives the confidence and reassurance that you can use email freely on a day-to-day basis, without the risk or concern associated with email threats.

How does it work?

Our Email Protection solution uses sophisticated detection engines and the latest threat intelligence to scan emails for threats, suspicious content, and anomalies.



Fraud and content checks

CORVID Email Protection scans every email against a series of fraud detection and content checks, to verify its legitimacy and level of risk. Our checks can be grouped into three categories:

Malware

- **Malware content** – checks for attached or embedded malware.
- **File type** – checks for known bad file types.
- **Active content** – Microsoft Office documents and PDF files containing macros are checked for behaviour which is commonly used to stage the download of malware (e.g. Emotet).

Impersonation

- **Domain impersonation** – is the email from the domain it appears to be from? Techniques such as substituting adjacent letters and replacing similar letters are used to make the domain look legitimate at a glance.
- **Trusted source** – is the email from one of the known source IPs that are registered for that domain?
- **VIP spoofing** – is the email from the VIP it claims to be from? The display name is often spoofed to make an email appear as if it came from a VIP known to you. Your company's VIPs can be registered in CORVID Email Protection, so the email is flagged if it claims to be from one of them but isn't.
- **Previous email activity with sender** – have you emailed this person before, or has anyone else in your company?
- **Punycode (IDN) detection** – has Punycode been used to make the email look like it's from a genuine source?
- **Reply redirection** – will your reply go to a different email address to the one that's displayed?

Malicious content/URLS

- **Secure transfer** – was the email received over an encrypted channel?
- **Domain age** – was the email sent from a newly-created domain? New domains are often used to spoof legitimate domains, and to send spam.
- **Spam identification** – is the email spam?
- **Decode short URLs** – URL shorteners can be used to evade the checks performed on URLs. CORVID Email Protection follows shortened links to check the actual destination is a genuine and trusted one.
- **Encrypted archive protection** – password-protected documents can't be scanned, but sharing the document password securely with CORVID Email Protection allows our system to scan the attachment for malicious content, while keeping the content and password confidential.

These checks carry out a comprehensive assessment of each email that passes through CORVID Email Protection, ensuring all potential areas of compromise are covered. This gives you peace of mind that the email you see in your inbox is not a threat to your device or network.

Once our checks have been carried out, CORVID Email Protection assigns a banner to each email, and sends it to your inbox.

CORVID banner

The CORVID Email Protection banner appears on every email you receive. It uses a simple traffic light rating system (red, amber, and green), so you can be confident of the nature of each email at a glance.

- **Red** – this banner provides the highest level of alert, making sure your attention is drawn to an issue that should not be ignored. If malware is attached to the email, it will be quarantined so it does not reach your inbox. You'll still receive an email with the red banner, but we will have removed the malicious content.
- **Amber** – our scans have found some areas of concern, which will show as warning messages in the banner, but CORVID Email Protection has deemed the email safe enough to be sent to your inbox.
- **Green** – the scans haven't found any issues, and the email appears to be legitimate.

Warning messages can be customised to suit your organisation's needs.

The banner displays three links to help you manage your emails:

1. **View email info** – an in-depth analysis of your email, including where it came from, and a detailed explanation of any issues identified.
2. **View all emails** – click this link to access the Email Manager.
3. **Report as suspicious** – if you receive an email you think may include suspicious content, click this link to send details to us, so we can investigate.

Take a look at the CORVID Email Protection user guide for full details of the warning messages the banner can display.

Email Manager

CORVID Email Manager is a web interface where you can manage your protected emails. You can review emails you've received, recover deleted emails, resend emails to your inbox, and release emails that have been blocked.

Encrypted attachments are commonly used by attackers to bypass security mechanisms. To deal with this problem, you could either permit encrypted attachments and rely on users being able to identify the difference between a malicious and benign attachment, or block encrypted files, meaning sensitive information needs to be released by the IT administrator, whether they have a need to know the information or not. Neither situation is a good one.

CORVID Email Protection allows you to submit passwords for encrypted files, meaning you can retain confidentiality without compromising security or needing to understand every sophisticated type of malware. Our system uses the password to automatically decrypt the file, scan it, then release it if it's safe – all without administrators being involved, and without security being compromised.

There's no need to remember another username and password for Email Manager – you reach it via a one-time access token link, which expires after 15 minutes. If your session times out, you can simply request another link.

Take a look at the Email Manager section of the user guide for more information.

CORVID Email Manager has two levels of access:

- **User** – users can view emails, manage document passwords, view the user guide, and access support. Users only have access to their own content.
- **Domain administrator** – in addition to the user permissions, domain administrators have access to the dashboard, can customise banner warnings, whitelist new and trusted domains, and access all content for associated domains.

System requirements

There are no specific system requirements to use CORVID Email Protection – all you need to do is change two email records (MX and SPF) to point at our solution. It integrates seamlessly with multiple email providers, such as Mimecast, Office 365, Exchange, and the G-suite, as well as any existing on-premise email solution you have.

Key business benefits

- **Remove reliance on users** – our traffic light security banner gives an instantly visible indicator as to the legitimacy of each email, so users don't have to make the decision on whether or not trust it.
- **Dramatically reduce user training** – you no longer need to provide training on how to identify the latest threats, as the intuitive, easy to use system does it automatically.
- **Up-to-date protection for your IT estate** – the system keeps pace with the latest threats through timely, accurate, and actionable intelligence from CORVID's cyber security experts. Multiple, sophisticated detection engines and threat intelligence sources ensure near real-time email security and protection.
- **Preserve data confidentiality** – users manage their own password-protected documents, so attachments are kept between users – your IT administrator doesn't need to get involved.
- **Effortless installation and integration** – a typical implementation takes less than five minutes. The highly scalable, 100% cloud-based service integrates with a wide range of mail servers, without delays in email delivery.
- **Peace of mind for you and your business** – the intelligent email security system filters unwanted emails, protects your business from attacks, and keeps your users safe.

About CORVID

We're an experienced team of cyber security experts, developers and analysts who are passionate about delivering innovative, robust and extensive cyber defence solutions and services to help protect businesses against cyber threats.

Get in touch

Get in touch to find out more, and discover how CORVID Email Protection can help your business.

CALL US
+44 1242 651251

EMAIL US
contact@corvid.co.uk

VISIT US
www.corvid.co.uk

FIND US

Arle Court, Hatherley Lane, Cheltenham, Gloucestershire, England, GL51 6PN

CORVID