



# CORVID BROKER

Keep full control of your IT and information, while CORVID monitors your cyber defences

Many Managed Detection and Response services require full access to, and visibility of, your entire IT estate, which we know is a daunting prospect and comes with its own set of security risks. With CORVID's broker, you can ensure your organisation is always in complete control of your sensitive data, while [CORVID Managed Detection and Response](#) monitors your systems.

## Keep your sensitive data secure

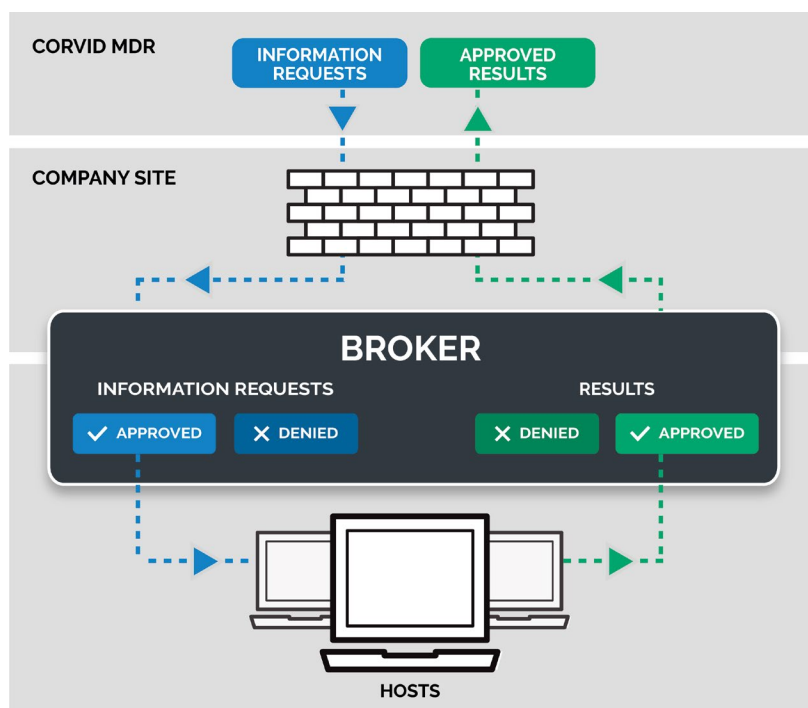
We understand the importance of cyber security. We live and breathe it. To allow our analysts to maximise your cyber defence capability, they need to extract specific information from your IT systems, such as system logs, file access information, and other metadata for detailed analysis. But it's exceedingly rare that our analysts need to read your business information and company files, so we devised an information broker that puts you in control at all times of what information we can access. This means you control your information while we protect your systems.

## What is the broker?

The CORVID broker is a unique, on-premise or cloud-based appliance that mediates all information exchanges between CORVID and your systems.

It keeps a comprehensive audit log of every single piece of information CORVID has sent and received, so you can see which data has been accessed and when – more than enough to satisfy even the most demanding of auditors, and ensure adherence to strict compliance regulations, such as GDPR.

With it, you can set rules regarding what types of information can be accessed by the CORVID agent, or what processes and activities can be run on hosts. You can even have different levels of access based on different hosts, because one size rarely fits all.



## How is it managed?

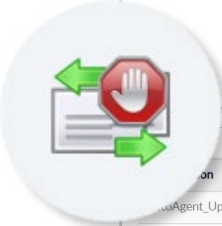
If you decide to change the default settings, you can fully manage and configure the broker using our intuitive web portal interface. You can control:

- the types of information CORVID analysts can access (by file type and/or description)
- whether you need to manually approve extraction of certain types of information, or the running of specific commands on a host
- if CORVID can examine potentially malicious files

Each unique combination of task and host can be managed individually, using the Permission Manager. You can set the following rules for each combination:

- **NOT SET** – rule has not yet been applied (this is the default setting for all rules).
- **ALLOW** – information requests will always be allowed.
- **MANUAL** – each request requires manual inspection before being allowed or denied.
- **DENY** – information requests will always be denied.
- **HOST-SPECIFIC** – this is only for results files. For example, results from some PCs could be automatically allowed to return to CORVID, whereas results from some server machines could be subject to manual inspection before being allowed or denied.

You can set or change rules in bulk using the 'All permissions' drop-down. Permission Manager also allows you to set permissions by file type, if you know you'll always assign the same rule to a certain type of file.



**PERMISSION MANAGER**

Set rules to control the processing of requests and results according to the invoked permission

< Previous Page 1 of 3 Next > Last >] Rows per page: 10 ?

Permission	Description	Request Status	Result Status
HostAgent_Update	Allow the host agent software to be updated.	Manual	Manual
AutostartMetadata_Read	Allow the enumeration of metadata about auto-start programs.	Allow	Manual
ConfigFiles_Read	Allow system configuration files to be read.	Allow	Manual
DNSMetadata_Read	Allow the enumeration of metadata about the systems DNS activity.	Allow	Manual
DiskMetadata_Read	Allow the enumeration of metadata about the systems hard disk drive.	Allow	Manual
DocumentMetadata_Read	Allow the enumeration of metadata about user documents.	Allow	Manual
Document_Acquire	Allow user documents to be acquired.	Allow	Manual
Document_Read	Allow user documents to be read.	Allow	Manual
EventLogs_Read	Allow system event logs to be read.	Allow	Manual
MemoryFiles_Read	Allow files in live memory to be enumerated.	Allow	Manual

Set request status of all permissions to: Please Select

Set result status of all permissions to: Please Select

Each time the rule matrix is saved, the broker automatically takes a point-in-time snapshot. You can review the full timeline of historical snapshots, giving you complete oversight of what was changed and when. This means not only can you audit what CORVID does to provide cyber defence, but you can also audit what settings were in place at any time in the past.

## Information flow between CORVID and your systems



CORVID creates a request for information, detailing the activity and why it's being requested.



All information requests go into the 'Information requests inbox', which works just like your normal email client, where you can approve or deny requests.



If a request includes an activity you think is too sensitive for CORVID to access, you can deny the request, so it doesn't get sent to the host



Your hosts regularly check in with the broker to see if an approved information request is available. They then carry out the task(s), and return a results file.



The broker processes results files according to the rules you've set. Just like inbound information requests, results files are sent to a 'Results inbox' for you to approve or deny, keeping you in control of everything that goes out as well as everything that comes in.

Take a look at our [user guide](#) for full details of how the broker works.

## Analysis and management

The web portal allows you to fully manage all aspects of your broker.

- Statistical analysis about information and requests – you can change the date range displayed here to show custom data, which can help with your reporting requirements.
- User account management – reset your password, and add, edit, or delete user accounts.
- Broker maintenance – your broker administrator can view and implement diagnostic and analysis commands for the broker, which can be run at any time.
- Advanced administration – get a full view of all your audit logs.

## Key business benefits

- ✓ Our broker has been inspected and approved for use by the U.S. Department of Defense, giving you peace of mind that it's a reliable service you can trust.
- ✓ Retain total control of your IT and information, while CORVID monitors your defences.
- ✓ Either a dedicated on-premise appliance or a cloud-service, enabling you to comply with complex security accreditation regulations, and meet demanding InfoSec requirements.
- ✓ Complete transparency of all inbound and outbound requests.
- ✓ Clear and comprehensive audit logs, to help you meet legal and regulatory rules.
- ✓ Up-to-date security – we release patches to improve performance, fix known issues, or combat a new type of cyber threat.

## About CORVID

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



CORVID was developed by Ultra Electronics, a FTSE 250 company, to safeguard its military, aerospace, and critical infrastructure data as well as that of its customers and supply chain. Ultra's pedigree enabled it to identify that traditional cyber defences were insufficient to combat the evolving complexity of threats – as a result, the CORVID initiative was started to provide a better and more comprehensive solution to the cyber problem. At the request of suppliers and business partners, it was decided to make CORVID available as a commercial solution to all organisations.

## Get in touch

Get in touch to find out more, and discover how CORVID's broker can help your organisation.

### CALL US

+44 1242 651251

### EMAIL US

[contact@corvid.co.uk](mailto:contact@corvid.co.uk)

### VISIT US

[www.corvid.co.uk](http://www.corvid.co.uk)

### FIND US



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

