



CRITICAL INFORMATION HEALTH CHECK

FAQ (Frequently Asked Questions)



Why undertake a Critical Information Health Check?

A Critical Information Health Check is a unique opportunity to discover if there are any gaps in an existing information security system where sensitive data is crossing an organisation's boundary unauthorised. With the new EU Data Protection Regulations almost upon us, those responsible for the security and protection of critical information at their organisation need to be 100% certain there are no gaps in their system, and therefore no risk of data breaches occurring.



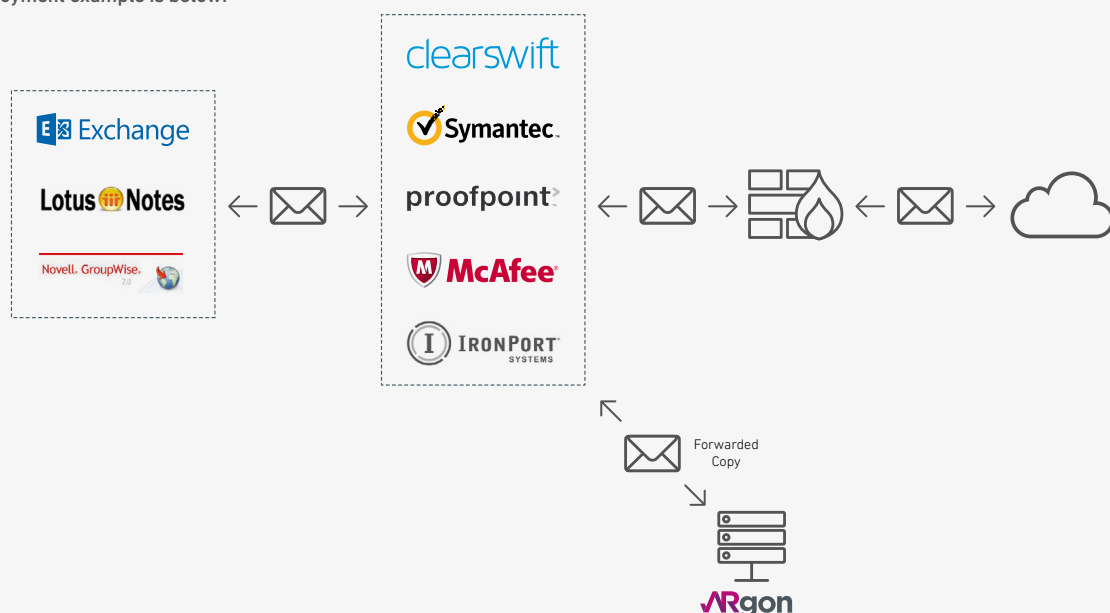
Do I really need to undertake a Health Check if we don't handle any sensitive information?

A Health Check will benefit any organisation, and often the less regulated industries provide the most surprising results. Whether it's company or customer confidential, private or personal, every organisation holds data that is sensitive to somebody inside its boundary. A Health Check will help you understand if any of this data is leaking across a boundary unauthorised and putting your organisation at risk of a data breach. It will also detect malware entering your organisation.

How does it work?

To perform a Health Check, Clearswift's ARgon for Email solution is deployed in an organisation's environment and will receive email over SMTP. Typically, ARgon will sit in what we refer to as 'out of line' so it's just 'monitoring' email. ARgon does not have an impact on mail flow at any stage, even when being deployed or if it fails for any reason.

A typical deployment example is below:





What Information are you looking for?

By default ARgon for Email will monitor information which is considered critical to most organisations like PCI information, PII information, active content and hidden data such as revision history and metadata attached to files. However, the search can be expanded to cover other structured data, so just let us know if there is anything else you would like to monitor.



What do you do with the information you monitor?

At the end of the Health Check some high level reports will be run that do not contain any identifiable information, but rather the number of incidents for the data we are monitoring presented in graph format. Depending on how the Health Check is configured, we can hold a copy of the information found for further analysis - if you would like us to do this, just let us know.



What happens if sensitive information is inadvertently uncovered when running the report?

If we do uncover any sensitive information as a result of the Health Check, we will notify you at the earliest opportunity. Any processing of personal, sensitive or confidential data will be carried out with guidance from you and/or in accordance with any applicable legal requirements. In particularly sensitive environments, we can instruct you on how to run the high level reports yourself if you would prefer.



How is it deployed?

ARgon for Email can be installed in the following ways:

- As a physical appliance provided by Clearswift
- As a virtual appliance on VMWare or Hyper-V
- As a 'soft' appliance – installed on your own hardware

Regardless of how ARgon for Email is installed, the ARgon gateway is configured with network settings through an initial wizard – then configuration and reporting is carried out through a web UI over HTTPS.



How long does it take?

Typically the Health Check will run on your environment for 2-3 weeks, though this can vary depending on your requirements. We will endeavour to create the report as soon as possible at the conclusion of the Health Check, but you should allow between 1-2 weeks for the Critical Information Health Check Report to be delivered to you.



What does the report look like?

Reports are typically customised based on the incidents that are uncovered but we do have a sample report available which is very similar to what you will receive. Just let us know if you would like a copy.



What do I need to do technically?

We realise that assigning resource to a Health Check could be challenging, so we endeavour to handle as much of the process as possible. In simple terms, we will only need your assistance for the following:

- Deploying a virtual machine or physical appliance/server
- Supplying us with network settings to be applied
- Configuring the firewall to allow communications
- Configuring the existing MTA to forward/relay a copy of all/selective messages as preferred