

# RANSOMWARE CONTAINMENT (RC)

## RC is a unique, new technology with advanced multi-layered detection and a completely different approach to prevention technologies

S10 Group turns detection into containment: detect malicious file behaviour, contain the infected user or device, and stabilise recovery with precise evidence and reporting.

RC monitors the current state of your documents on file level (e.g., xis, doc, pdf etc.). Every time someone creates a new file or overwrites an existing file, RC looks directly into the file through the multiple detection methods at work, spotting file changes and/or encryptions inside the data being saved. RC has a different methodology compared to what First Line of Defence solutions have. These solutions monitor malware coming from outside of the organization and prevent this malware from executing, but not checking if any encryption already has taken place. RC is a new, additional layer of protection for your organization. Therefore, if you copy a normal word file that has already been encrypted by ransomware to your network, RC will detect this. However, this would bypass any of your existing security solutions in place.

## DETECT

### Detailed live visibility with playback

RC creates a baseline of all the activity on your systems and in your environment. It simply monitors the network traffic, going to and from your network file servers, using heuristics and metadata to discover ransomware swiftly. Artificial Intelligence and Machine Learning automate the initial alert settings, making it even more sensitive based on your real network activity.

In seconds, RC provides you with full visibility of any live file changes on your entire network. It gives you visibility on the WEB Dashboard which displays the recording log of any file creation, change, rename or deletion, so in case of an attack, you know exactly which files have been compromised. Often, companies are astonished by the detailed overview of the file changes that take place within your organization as well as your premises abroad. In case of an attack, you have an advanced playback feature of the history log which makes you able to easily study all details related.

## CONTAIN / RESPOND

### Keep your organization running smoothly

RC will respond within seconds of any detected ransomware attack, shutting down the infected user/client and stopping any ransomware from spreading into the organization. RC will inform you as soon as the attack has been stopped, and the alert level has subsided to normal.

Integration through RESTful API to other security solutions such as Cisco ISE and Windows Defender ATP, means your security teams can unify security management across an increasingly complex sea of endpoints. RC will react within seconds of an unexpected file encryption taking place, alerting the Security Operations Centre (SOC) team, the attacked user, any other key stakeholders and finally notify the local GDPR Supervisory Authority (SA) if required.



Alerting is done by email, SMS, IOS/Android app and through integration with most STEM solutions. The alerting and communication also work if you are hosting in the cloud or having an MSP taking care of your IT solution and infrastructure history log which makes you able to easily study all details related.

No other security solution provides you with such detailed and structured overview

## STABILISE / RECOVER

Remove pressure from the operational team RC provides a speedy data-recovery concept. It gives you an exact list of the few files infected before the forced shutdown that needs to be restored from your backup. It will reduce any potential downtime by identifying the exact files that need to be recovered, saving you valuable time with minimal cost of recovery. Some of the latest tactics from the cyber criminals are encrypting files without even changing the file name as well as encrypting files in different folders across your infrastructure. This makes recovery difficult and ultimately forces you to restore a full backup and putting additional pressure on the entire organization with operational loss and potentially a GDPR headache. With RC your organization will safely and quickly be operational without having to pay the ransom.



## REPORT / EXPLAIN

### Automate your GDPR response when hit by ransomware

According to the GDPR regulations: "If it's likely that there will be a risk, then you must notify the local GDPR Supervisory Authority (SA); if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it"

Ransomware is an obvious tool of choice for cyber criminals, encrypting files on different shares and folders spread across the network, making GDPR reporting a challenge. Time pressure is now a serious issue, not only from the cyber criminals - but now you also only have 72 hours to comply with GDPR.

If you have a breach and have RC in place, it will mostly be a minor incident, but you still need to document your findings. RC provides a fully automated process for internal audit and for major breaches as RC:

Records the exact time of the attack (from beginning to end)

Tells where the attack was initiated (which endpoint)

Shows exactly which files have been affected

Reveals who the file owner is

Gives details of how and when the breach was stopped

Generates an incident report to key stakeholders

With RC's immediate response, most incidents will be considered minor, as only a few files will be compromised before a forced shut down. Customized GDPR reporting ensures you are compliant.