RansomWare Containment

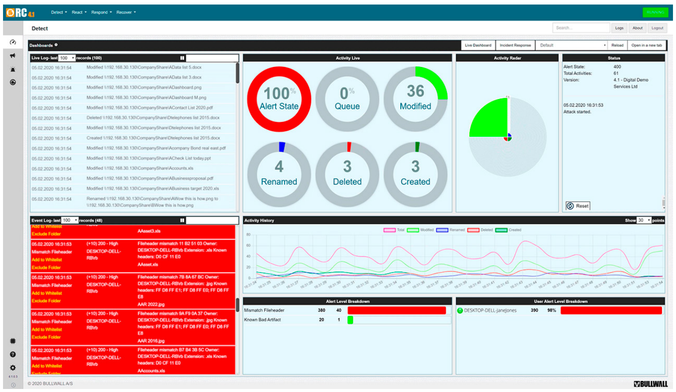
Our RansomWare Containment (RC) offering is a proven and automated containment solution, laser-focused on stopping any type of ransomware outbreak.

Criminals are innovating new and unknown methods continuously to defeat traditional signature-based methods of detection. It is critical that organizations do not rely solely on a reactive response to modern malware threats. Daily, we hear reports on how this strategy has proven to fail. Once the RansomWare is in and starts delivering its payload (encrypting your data), it matters less how it got in, and at this point, it is too late for your prevention-based security to react. At this point, it matters much more that you can stop the illegitimate encryption as fast as possible.

RC has a very different methodology to what the prevention-based solutions do and is a new and complementary layer of protection for your organization. Prevention-based solutions, such as Anti-virus, focus on preventing malware from executing by looking at the traffic coming into your organization. However, if RansomWare manages to circumvent and fool your existing security, it will encrypt up to 50.000 files per minute.

Do you trust that 100% prevention will work 100% of the time? The answer should be no, simply because these solutions focus on threat detection and protection, but have no ability to stop ongoing illegitimate encryption. Prevention and protection are essential: but with RansomWare, it is crucial to detect, respond, and recover quickly.

Our innovative and agentless solution, is a new Last Line of Defence technology that detects RansomWare outbreaks in seconds by monitoring the organization's data activity. RC investigates the heuristics of each file accessed by a user either on-premise or in the cloud, without causing any network overhead.



Live Log- last 100 records (100)

```
05.02.2020 16:31:54   Modified \\192.168.30.130\CompanyShare\AData list 5.docx
05.02.2020 16:31:54   Modified \\192.168.30.130\CompanyShare\AData list 3.docx
05.02.2020 16:31:54   Modified \\192.168.30.130\CompanyShare\ADashboard.png
05.02.2020 16:31:54   Modified \\192.168.30.130\CompanyShare\ADashboard M.png
05.02.2020 16:31:54   Modified \\192.168.30.130\CompanyShare\AContact List 2020.pdf
05.02.2020 16:31:54   Deleted \\192.168.30.130\CompanyShare\Dtelephones list 2015.docx
05.02.2020 16:31:54   Modified \\192.168.30.130\CompanyShare\Dtelephones list 2015.docx
05.02.2020 16:31:54   Created \\192.168.30.130\CompanyShare\Dtelephones list 2015.docx
05.02.2020 16:31:54   Modified \\192.168.30.130\CompanyShare\Acompany Bond real east.pdf
05.02.2020 16:31:54   Modified \\192.168.30.130\CompanyShare\ACheck List today.ppt
05.02.2020 16:31:54   Modified \\192.168.30.130\CompanyShare\Accounts.xls
05.02.2020 16:31:54   Modified \\192.168.30.130\CompanyShare\ABusinessproposal.pdf
05.02.2020 16:31:54   Modified \\192.168.30.130\CompanyShare\ABusiness target 2020.xls
05.02.2020 16:31:54   Renamed \\192.168.30.130\CompanyShare\AWow this is how.png to
                      \\192.168.30.130\CompanyShare\BWow this is how.png
```

Alert State:	400
Total Activities:	61
Version:	4.1 - Digital Demo Services Ltd

05.02.2020 16:31:53
Attack started.

Event Log- last 100 records (48)

```
Add to Whitelist
Exclude Folder                                        AAsset3.xls

05.02.2020 16:31:53   (+10) 200 - High   Fileheader mismatch 11 B2 51 03 Owner:
Mismatch Fileheader   DESKTOP-DELL-      DESKTOP-DELL-RBvb Extension: .xls Known
Add to Whitelist      RBvb               headers: D0 CF 11 E0
Exclude Folder                           AAsset.xls

05.02.2020 16:31:53   (+10) 200 - High   Fileheader mismatch 7B 8A 67 BC Owner:
Mismatch Fileheader   DESKTOP-DELL-      DESKTOP-DELL-RBvb Extension: .jpg Known
Add to Whitelist      RBvb               headers: FF D8 FF E1; FF D8 FF E0; FF D8 FF
Exclude Folder                           E8
                                         AAR 2022.jpg

05.02.2020 16:31:53   (+10) 200 - High   Fileheader mismatch 9A F9 0A 37 Owner:
Mismatch Fileheader   DESKTOP-DELL-      DESKTOP-DELL-RBvb Extension: .jpg Known
Add to Whitelist      RBvb               headers: FF D8 FF E1; FF D8 FF E0; FF D8 FF
Exclude Folder                           E8
                                         AAR 2016.jpg

05.02.2020 16:31:53   (+10) 200 - High   Fileheader mismatch B7 B4 3B 5C Owner:
Mismatch Fileheader   DESKTOP-DELL-      DESKTOP-DELL-RBvb Extension: .xls Known
Add to Whitelist      RBvb               headers: D0 CF 11 E0
Exclude Folder                           AAccounts.xls
```

Alert Level Breakdown		
Mismatch Fileheader	380	40
Known Bad Artifact	20	1

User Alert Level Breakdown		
DESKTOP-DELL-JaneJones	390	98%

DETECT: DETAILED LIVE VISIBILITY

RC creates a baseline of all the file activity on your systems and in your environment. It simply monitors the network traffic from your network file servers, using heuristics and metadata to detect RansomWare swiftly.

Artificial Intelligence and Machine Learning automate the initial alert settings, making it even more sensitive based on your real network activity. Companies are often astonished by the detailed overview of the file changes within their organization. In case of an outbreak, you have an advanced playback feature of the history log, which allows you to study all details easily.

RESPOND: KEEP YOUR ORGANIZATION RUNNING

On detecting illegitimate encryption, RC immediately raises an alert, and a response is triggered to shut down the endpoint that is causing the illegitimate encryption outbreak.

Encryption stops instantly, before it spreads to the rest of your organization, becoming a very costly affair. There is a wide range of isolation methods that can be utilized, such as disable VPN, disable AD-user, disable NAC, and forced shutdown.

Alerting is done via email, SMS, and through integration with most SIEM solutions. The alerting and communication also works if you are hosting in the cloud or having an MSP taking care of your IT solution and infrastructure.

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.

RECOVER: PROVIDES THE FULL OVERVIEW

RC provides a speedy data-recovery concept. It gives you a detailed 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 recovery costs.

HASSLE-FREE INSTALLATION

RC is an agentless solution and is not installed on endpoints or any existing servers or file servers. There is no impact on endpoints and no network performance issues. Agentless file behavior monitoring and machine learning techniques are deployed with ease in less than a day, and RC is configured automatically.

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

RC monitors the current state of your documents on file level (e.g., xls, 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 Defense solutions have. These solutions monitor malware coming from outside of the organization and prevent these 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 automates the initial alert settings, making it even more sensitive based on your real network activity.

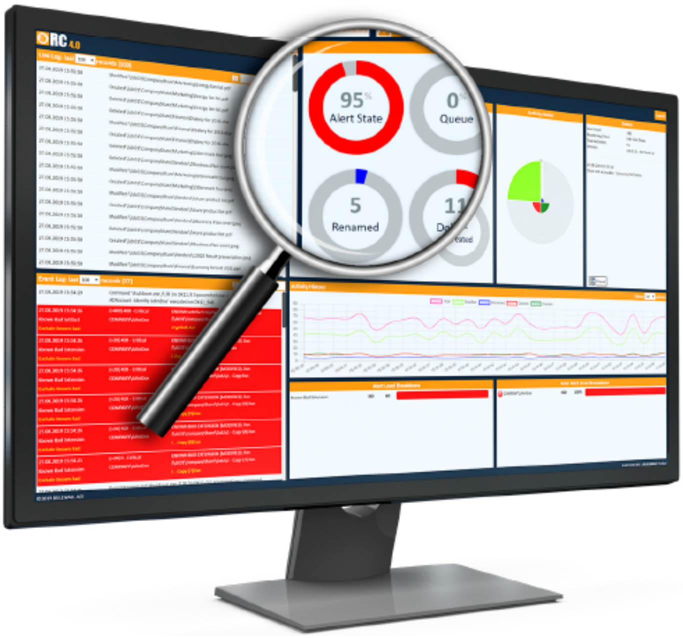
In seconds, RC provides you with full visibility of any live file changes on your entire network. It gives you visibility on the WEB Dashboard which displays the recording log of any file creation, change, rename or deletion, so in case of an attack, you know exactly which files have been compromised. 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.

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 works 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.

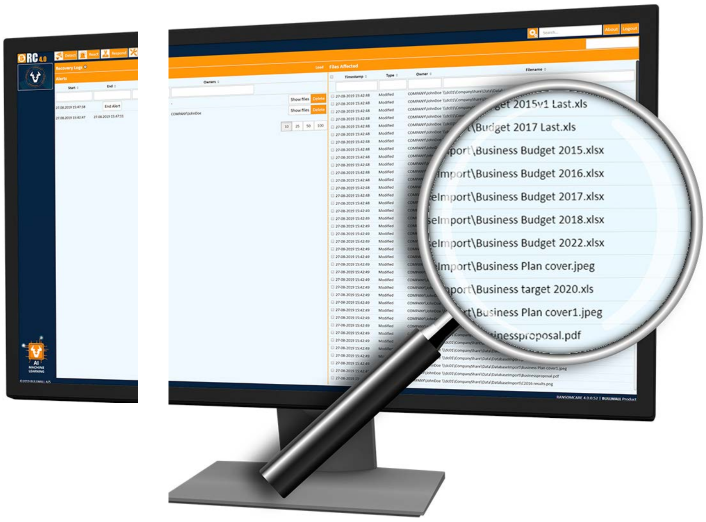
RECOVER

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.


RC 4.0
get 2015v1 Last.xls
Budget 2017 Last.xls
port\Business Budget 2015.xlsx
mport\Business Budget 2016.xlsx
elmport\Business Budget 2017.xlsx
elmport\Business Budget 2018.xlsx
elmport\Business Budget 2022.xlsx
mport\Business Plan cover.jpeg
port\Business target 2020.xls
t\Business Plan cover1.jpeg
inessproposal.pdf

REPORT

Automate your GDPR response when hit by ransomware

According to the GDPR regulations: "If its likely that there will be a risk, then you must notify the local GDPR Supervisory Authority (SA); if its 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 effected
- 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.