STOP RANSOMWARE BEFORE IT STOPS YOU

HOW DO YOU KNOW THAT YOU ARE UNDER ATTACK?

In a scenario where a ransomware has already bypassed your existing security solutions, it is now effectively “whitelisted” to attack your business, causing as much disruption as possible by encrypting as many of your files as it can in the shortest possible time.

Why is RC (RansomCare) different?
RC is a new and innovative technology that from a central server installation (Agentless), detects ransomware attacks by looking into the heuristics of your actual data files from i.e. word, excel, pdf. etc., stored on your entire storage platform and in the cloud.

- **How do you** see which files are encrypted and where they reside?
- **How do you** identify which user and which device initiated the attack?
- **How do you** stop the ongoing encryption immediately before significant damage occurs?
- **How long** will it take you to restore hundreds of thousands of files and what is the total cost of downtime?
- **What amount** of time is needed to accurately report GDPR if thousands of files with personal information has been lost to illegitimate encryption?

Why Ransomware Should Matter to You

Ransomware has evolved into enterprise-grade malware that holds computers and data files hostage, locks down entire systems swiftly, and brings business to a halt for days to months on end. And criminals are innovating new unknown methods continuously to defeat traditional signature-based methods of detection. Now more than ever, the C-suite (CIO, CISO CFO and CEO) has a significant stake in securing data and intellectual capital to protect PII, revenue, maintain customer loyalty and secure shareholder value.

It’s critical that organisations don’t rely solely on a reactive response to modern malware threats. On a daily basis we hear reports on how this strategy has proven to fail. The future defence strategy needs to include business continuity and disaster recovery with a Last Line of Defence solution which enables automatic alerting, shutdown response and quick recovery without the vast costs often associated with ransomware attacks.

How does it work

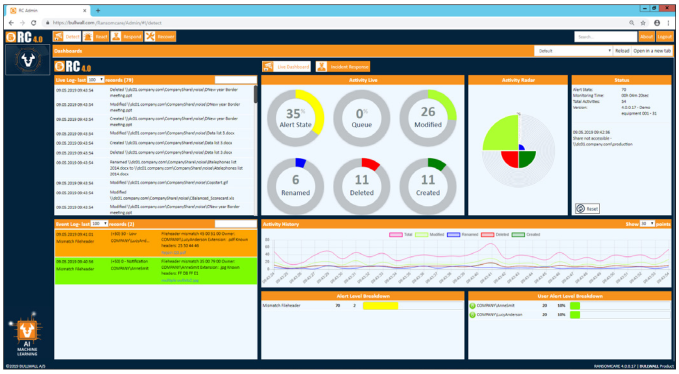
RC will detect and stop ransomware attacks, even when the malware has bypassed all your existing endpoint protection and other prevention or behavioural security tools. It is a vital element of your overall defence strategy, providing critical security defence for a small portion of your available security budget.

RC provides a revolutionary Last Line of Defence against the threat from ransomware. With a rapidly expanding attack surface to defend and multiple entry points for malware into organisations today, RC delivers a 24/7 automated response. It does not matter which user, or which device triggered the attack. Nor does it matter if it is a known or unknown ransomware attack, or if the attack started on an endpoint, a mobile phone, an IOT device, via email, website drive-by-attack, instant messaging apps, USB key, download, or were deployed by someone inside your organisation.

When RC detects a ransomware attack, an alert is raised instantly and a response can be triggered to shutdown the endpoint under attack (Windows, Mac and Linux) so encryption stops instantly. RC also handles virtual environments like Citrix servers/sessions, Terminal servers/sessions, Hyper-V, VMware and the Cloud including Azure and Amazon AWS/EC2, Sharepoint, Google Drive and Office 365. RC disables and stops the device encrypting your data including mobile devices.

Hassle free installation

RC is an agentless solution and is NOT installed on endpoints or any of the existing servers or file servers. There is no impact on endpoints and no network performance issues. Agentless file behaviour monitoring, and machine learning techniques are deployed with ease in 4 to 6 hours, and RC is configured automatically. Full integration to other security solutions like Cisco ISE and Windows Defender ATP or SIEM system are available via RESTful API allowing your security teams to unify security management across an increasingly complex sea of endpoints.



Live Log- last 100 records (79)

09.05.2019 09:43:54 Deleted \\dc01.company.com\CompanyShare\noise\DNew year Border meeting.ppt
09.05.2019 09:43:54 Modified \\dc01.company.com\CompanyShare\noise\DNew year Border meeting.ppt
09.05.2019 09:43:54 Created \\dc01.company.com\CompanyShare\noise\DNew year Border meeting.ppt
09.05.2019 09:43:54 Modified \\dc01.company.com\CompanyShare\noise\Data list 3.docx
09.05.2019 09:43:54 Created \\dc01.company.com\CompanyShare\noise\Data list 3.docx
09.05.2019 09:43:54 Deleted \\dc01.company.com\CompanyShare\noise\Data list 3.docx
09.05.2019 09:43:54 Renamed \\dc01.company.com\CompanyShare\noise\Btelephones list 2014.docx to \\dc01.company.com\CompanyShare\noise\Atelephones list 2014.docx
09.05.2019 09:43:54 Modified \\dc01.company.com\CompanyShare\noise\Copstart.gif
09.05.2019 09:43:54 Modified \\dc01.company.com\CompanyShare\noise\CBalanced_Scorecard.xls
09.05.2019 09:43:54 Modified \\dc01.company.com\CompanyShare\noise\CNew year Border meeting.ppt

Event Log- last 100 records (2)

09.05.2019 09:41:01 Mismatch Fileheader (+50) 50 - Low COMPANY\LucyAnd... Fileheader mismatch 45 00 51 00 Owner: COMPANY\LucyAnderson Extension: .pdf Known headers: 25 50 44 46 Rejoin Q3.pdf
09.05.2019 09:40:56 Mismatch Fileheader (+50) 0 - Notification COMPANY\AnneSmit Fileheader mismatch 35 00 79 00 Owner: COMPANY\AnneSmit Extension: .jpg Known headers: FF D8 FF E1 multiple outlets2.jpg

Alert State: 70
Monitoring Time: 00h 04m 20sec
Total Activities: 54
Version: 4.0.0.17 - Demo equipment 001 - 31

09.05.2019 09:42:36
Share not accessible - \\dc01.company.com\production

Mismatch Fileheader	70	2	

COMPANY\AnneSmit	20	10%	
COMPANY\LucyAnderson	20	10%	