RICOH
imagine. change.

Ricoh Ransomware Containment

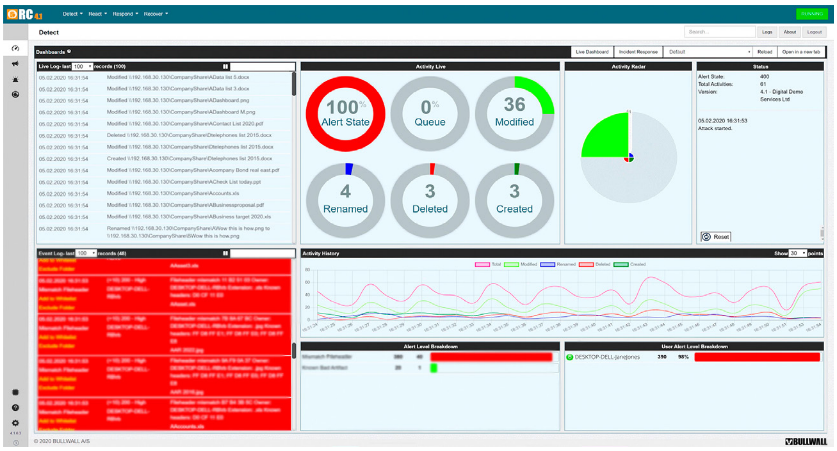
Ricoh's RansomCare offering is a proven and automated containment solution, laser-focused to stop malicious encryption on monitored file shares, securing critical data

Let's face facts: Even the most well-protected organisations fall victim to ransomware.
Cybercriminals are constantly developing new and innovative methods to defeat traditional, prevention-based detection methods. Ricoh's unique, agentless, multi-layered containment solution, RansomCare, powered by BullWall, stops illegitimate encryption and file corruption in its tracks. To stay safe from ransomware, an organisation must evolve its security defences and introduce a layered approach. Once ransomware has breached the network and begins delivery of its payload, it can be too late for existing security to react. At this point, the only thing that matters is how fast you can stop the illegitimate encryption from encrypting up to 10,000 files per minute.

Introducing the Ricoh Ransomware Containment solution, RansomCare: a unique and proven Last Line of Defence. Due to 20+ detection sensors, if illegitimate encryption is initiated by ransomware and files are corrupted on monitored file shares, RC reacts by isolating the compromised device and user to stop the illegitimate encryption process.

The offering is complementary to existing security defences. Traditional security defences focus on preventing malware from executing and protecting your organisation, should endpoints be the target of malware. But what if they fail? Ransomware is another story. It has crippled organisations even though they had the best-of-breed security solution in place. Organisations today should consider deploying a Last Line of Defence acting as the 'sprinkler system' should prevention-based security solutions fail.

RansomCare is considered a **Last Line of Defence technology**; it detects illegitimate file encryption and corrupted files on monitored file shares and cloud shares in seconds if existing security defences have failed to protect your organisation.



```
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.

DESKTOP-DELL-janejones 390 98%

Detect: Detailed Live Visibility

RC detects illegitimate encryption on monitored file shares in seconds by monitoring the organisation's data activity. It investigates the heuristics of each file accessed by a user either on-premise or in the cloud. By intelligently accumulating any detection of tell-tale signs of ransomware (encryption and corruption), RC will detect and respond to the active threat that existing security defences did not stop. Machine Learning automates the initial alert settings based on your actual data activity, tailoring them to your environment. Organisations are often astonished by the detailed overview of the file changes within their organsation, and in case of an outbreak, you can see the small number of files impacted before the forced isolation by RansomCare.

Respond: Contain and Stop The Outbreak

RansomCare reacts and responds once illegitimate file encryption is ongoing on monitored critical file shares, cloud shares (e.g., Google and O365 suite), or file server shares. It is crucial during ransomware outbreaks to detect, respond and recover as quickly as possible, as the financial and reputational repercussions caused by downtime can be costly. On detecting illegitimate encryption on monitored shares, RC immediately raises an alert, and a response is triggered to isolate the endpoint, device and/or user that is causing the illegitimate encryption on monitored file shares. A wide range of customisable isolation methods can be utilized, such as forced shutdown, disable VPN, disable AD-user, disable network access, and many others. Alerting is done via email, text, and through easy integration with all SIEM solutions. The alerting also works if you are hosting in the cloud or have an MSP taking care of your IT infrastructure. Integration through RESTful API to other security solutions means your security team(s) can unify security management across an increasingly complex sea of endpoints.

Recover: Provides the Full Overview

RansomCare provides a speedy data recovery concept. It provides a detailed list (for restoration purposes) of the small number of affected files before the forced isolation or shutdown. This reduces potential downtime significantly as it identifies the exact small number of files that need to be recovered, saving you valuable time and minimal recovery cost.

Hassle-Free Installation and Deployment

RansomCare 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.

Next Steps

You can book a 45-60-minute online demonstration with Ricoh and/or a two-hour Ransomware Assessment. During the Assessment, we utilize a safe and controlled ransomware simulator to test RansomCare's response to ongoing corruption of files on your file shares and allow you to experience RC at work in your own environment. The test can also help you test if your existing defences have the same response.

For more information, please contact:
Steve Timothy: steve.timothy@ricoh.co.uk
Colin Lock: colin.lock@ricoh.co.uk

RICOH
imagine. change.

CYBER ESSENTIALS
CYBER ESSENTIALS PLUS
iSF Information Security Forum
CREST

BULLWALL