Immediate Ransomware Isolation

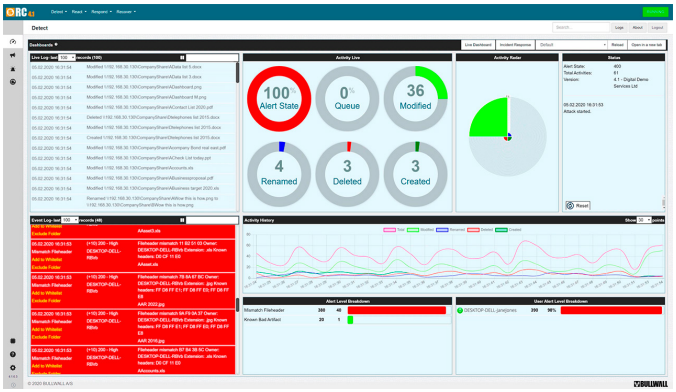
Our RansomCare offering is a proven and automated containment solution, laser-focused on stopping any type of ransomware outbreak.

Criminals are innovating new and unknown methods continuously to defeat traditional signature-based methods of detection. It is critical that organisations 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.

RansomCare (RC) has a very different methodology to what the prevention-based solutions do and is a new and complementary layer of protection for your organisation. 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 10,000 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, RC, is a new Last Line of Defence technology that detects Ransomware outbreaks in seconds by monitoring the organisation'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.



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 easily study all details.

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 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 recovery cost.

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 behavior monitoring and machine learning techniques are deployed with ease and RC is configured automatically.

BullWall A/S · Oester Snedevej 15 · 7120 Vejle East · Denmark | BullWall Ltd · 8 The Courtyard · Furlong Road · Bourne End · Bucks SL8 5AU · England