RICOH
imagine. change.

Ransomware Containment & Isolation



An automated solution to stop a ransomware outbreak within your organization

Let's face facts: Even the most well-protected organizations fall victim to ransomware. Cybercriminals are constantly developing new and innovative methods to defeat traditional, prevention-based detection methods. To stay safe from ransomware, an organization must evolve its security defenses and introduce a layered approach. Once ransomware triggers its payload (encryption), it may 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 of up to 10,000 files per minute.

A layered approach includes a complementary solution to detect and stop illegitimate encryption once it is ongoing. It can do that by monitoring the file activity on monitored file- and cloud shares. As soon as it sees ongoing criminal encryption and file corruption, it reacts and isolates the user causing it.

Introducing the Ricoh ransomware containment solution, RansomCare (RC) by BullWall, a unique and proven layer of defense. Over 20 detection sensors assess each file change on monitored shares. If the tell-tale signs of ransomware (illegitimate encryption) are initiated, and files are actively being encrypted on monitored file- and cloud shares, RC reacts by isolating the compromised device and user to stop the criminal encryption process. It is a vital element of your overall defense strategy, providing critical security defense for a small portion of your available security budget.

Can you answer these questions in the event of a ransomware outbreak?

- How do you see which files are encrypted and where they reside?
- How do you identify which user and which device is encrypting files?
- How do you stop the ongoing encryption quickly 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 to data authorities if thousands of files with personal information have been illegally encrypted?

www.ricoh-usa.com/ransomcare

Why Ransomware Matters

Now more than ever, the C-suite (CIO, CISO, CFO, and CEO) has a significant stake in securing data and intellectual capital to protect personally identifiable information (PII), revenue, maintain customer loyalty, and secure shareholder value. Traditional security defenses focus on preventing malware from executing and protecting your organization, should endpoints be the target of malware. But what if they fail? Ransomware is another story. It has crippled organizations even though they had the best-of-breed security solution in place. Organizations today should consider deploying an additional line of defense acting as the 'sprinkler system' should prevention-based security solutions fail.

It's critical that organizations don't rely solely on a reactive response to modern malware threats. Daily we hear reports on how this strategy has proven to fail. The future defense strategy needs to include business continuity and disaster recovery with a solution, enabling automatic alerting, shutdown response, and quick recovery without the vast costs often associated with ransomware attacks.

How it works

With a rapidly expanding attack surface to defend and multiple entry points for malware into organizations today, RansomCare delivers a 24/7 automated containment response to ransomware outbreaks with built-in response and reporting. It does not matter which user or which device triggered the encryption. Nor does it matter if it is a known or unknown ransomware variant or if the outbreak started on an endpoint, a mobile phone, an IoT device, via email, USB, or were deployed by someone inside your organization. RC investigates the heuristics of each file accessed by a user on monitored file shares either on-premise or in the cloud, without causing any network overhead. When RansomCare detects ongoing encryption and file corruption on monitored shares, an alert is raised instantly, and a response is triggered to disable and isolate the device and user encrypting your data.

RansomCare also works in 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 Microsoft 365. A wide range of customizable isolation methods can be utilized, such as forced shutdown, disable VPN, disable AD-user, disable network access, revoke cloud permissions, and many others. Integration through RESTful API to other security solutions means your security teams can unify security management across an increasingly complex sea of endpoints.

Hassle free remote installation

RansomCare is an agentless solution and is not installed on endpoints or existing servers, or file servers. There is no impact on network performance. Agentless file behavior monitoring and machine learning techniques are deployed with ease in 4 to 6 hours, and RansomCare will be configured according to your environment. RC features Cloud Connectors for organizations utilizing Microsoft O365 (SharePoint, Teams, OneDrive) and Google Drive. Full integration to other security solutions like Cisco ISE and Windows Defender ATP or SIEM system is available via RESTful API allowing your security teams to unify security management across an increasingly complex sea of endpoints.

- **No Cloud Installation**
- **No Endpoint Installation (agentless)**
- **No File Server / Storage Installation**

Alerts and Integrations

RansomCare built-in alerting services
Email Notifications
SMS Alert
Mobile "SOC"
API to other systems

2-Way Interface to Restful API (pre-configured scripts)
Splunk
Cisco ISE
Windows Defender
Aruba
IBM Radar
McAfee
Symantec
TrendMicro
ForeScout
and many others ...

Ransomware Assessment Test

Ricoh and BullWall can perform a Ransomware Assessment Test where a safe and controlled ransomware simulator is used to simulate zero-day file encryption and rapid file changes. We will then test RansomCare in your environment to demonstrate how the solution responds to an outbreak of file encryption. Ask a sales representative for more information.

This document is for informational purposes only and this document and any related services or products described herein are not intended to provide any legal, regulatory, compliance, or other similar advice. You are solely responsible for ensuring your own compliance with all legal, regulatory, compliance, or other similar obligations. While care has been taken to ensure the accuracy of this information, Ricoh makes no representation or warranties about the accuracy, completeness or adequacy of the information contained herein, and shall not be liable for any errors or omissions in these materials. Actual results will vary depending upon use of the products and services and the conditions and factors affecting performance. The only warranties for Ricoh products and services are as set forth in the express warranty statements accompanying them.

R4049

RICOH
imagine. change.