Ransomware Containment

Powered by BullWall RansomCare (RC)

RICOH
imagine. change.

An automated solution to stop a ransomware outbreak within your organization

Ransomware has evolved into enterprise-grade malware that holds computers and data files hostage, locks down entire systems swiftly, and brings businesses to a halt for days to months on end. 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. You will either pay the bad actors/attacker to get the files back, with no guarantee they will give it to you, or you will lose the data forever.

RansomCare 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 (i.e., word, excel, pdf. etc.) stored on your network and in the cloud.

RansomCare will detect and stop ransomware attacks, even when the malware has bypassed all your existing endpoint protection and other prevention or behavioral security tools. 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 & 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 an attack as per GDPR if thousands of files with personal information have been lost to illegitimate encryption?

Why Ransomware Should Matter

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. Cyber criminals are innovating new unknown methods continuously to defeat traditional signature-based methods of detection.

It is critical that organizations don't rely solely on a reactive response to modern malware threats. Everyday 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 Last Line of Defense solution that enables 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 reporting for compliance regulations such as GDPR. 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 organization.

When RansomCare 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. RansomCare 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 Microsoft 365. RansomCare disables and stops the device encrypting your data including mobile devices.

Hassle free remote installation

RansomCare 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 in 4 to 6 hours, and RansomCare 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.

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

Alerts and Integrations

RansomCare built-in alerting services
- Email Notifications
- WhatsApp Notifications
- SMS Alert
- Mobile "SOC"
- API to another system

2-Way Interface to RESTful API
(pre-configured scripts)
- Splunk
- Cisco ISE
- Windows Defender
- Aruba
- IBM Radar
- McAfee
- Symantec
- TrendMicro
- ForeScout

Ransomware Assessment Test

Ricoh can perform a ransomware assessment test to see if your existing security solutions can stop illegitimate encryption using a safe ransomware simulation tool. We will then test RansomCare meant to demonstrate how the solution responds to an outbreak. Ask a sales representative for more information.

RICOH
imagine. change.