SHUT DOWN RANSOMWARE BEFORE IT SPREADS

An automated solution to stop a ransomware outbreak within your organisation

Let's face facts: Even the most well-protected organisations fall victim to ransomware. Cybercriminals are constantly developing new and innovative ways to defeat traditional, prevention-based detection methods. To stay safe from ransomware, an organisation must evolve its security defences and introduce a layered approach. Once ransomware triggers its payload (encryption), it may be too late for existing security to react. At this point, what 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 file- and cloud shares. As soon as the solution identifies ongoing criminal encryption and file corruption, it reacts and isolates the user causing it.

Introducing the Ricoh ransomware containment solution- RICOH RansomCare powered by BullWall- a unique and proven layer of defence. 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, RICOH RansomCare reacts by isolating the compromised device and user to stop the criminal encryption process. The solution is a vital element of your overall defence strategy, providing critical security protection 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?

RICOH
imagine. change.

Why Ransomware matters

Now more than ever, the C-suite (e.g. 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 defences focus on preventing malware from executing, should endpoints be the target of malware. But what if they fail? Ransomware is another story. It has crippled organisations despite having best-of-breed security solutions in place. Organisations today should consider deploying an additional line of defence to act as a 'sprinkler system' should prevention-based security solutions fail.

It's critical that organisations don't rely solely on a reactive response to modern malware threats. We hear reports daily on how this strategy has proven to fail. The defence strategy of the future must include business continuity and disaster recovery, to enable automatic alerts, a 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 organisations today, RICOH 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 the attack 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 was deployed by someone inside your organisation. RICOH RansomCare 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 RICOH 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.

RICOH 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 customisable isolation methods can be utilised, 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

RICOH RansomCare is an agentless solution and is not installed on endpoints, 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 four to six hours, and RICOH RansomCare will be configured according to your environment. RICOH RansomCare features Cloud Connectors for organisations that utilise 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

RICOH RansomCare built-in alerting services

Email notifications
SMS alert
Mobile "SOC"
API to other systems

2-Way Interface to Restful

Splunk
Cisco ISE
Windows Defender
Aruba
IBM Radar
McAfee
Symantec
TrendMicro
ForeScout
and many others

Ransomware Assessment Test

We 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 RICOH RansomCare in your environment to demonstrate how the solution responds to an outbreak of file encryption. Ask a sales representative for more information.

RICOH
imagine. change.