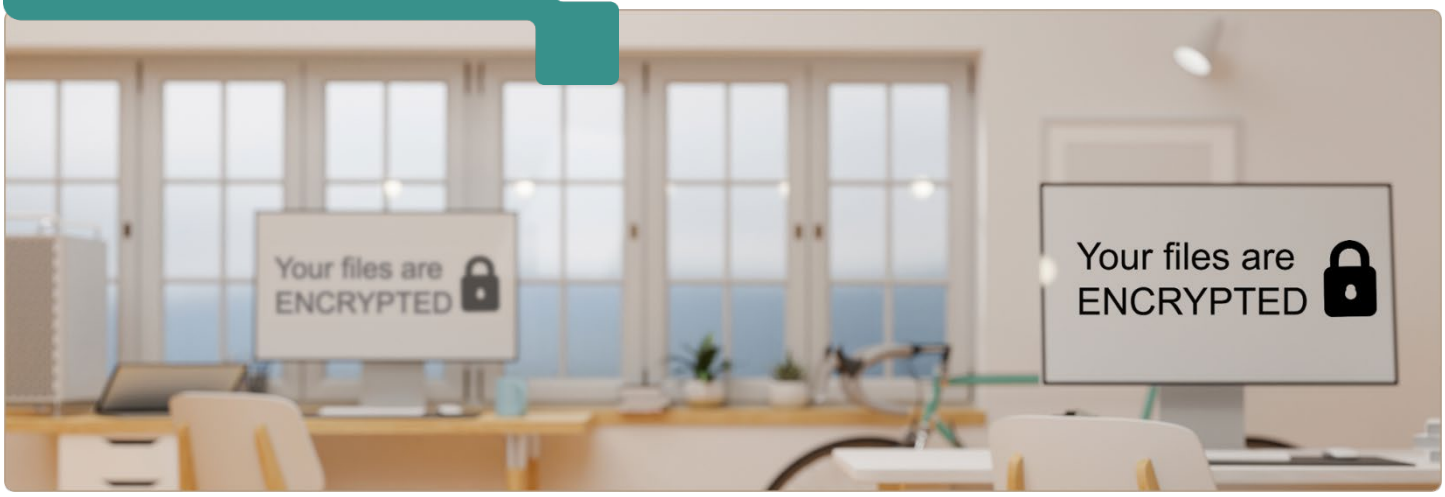
RansomCare:

Ransomware Containment

RICOH
imagine. change.



RansomCare: an additional line of defense that can stop a ransomware outbreak

Ransomware is malware that encrypts files, systems, and even networks for a ransom. Once it breaches a network perimeter defense it can encrypt an entire network - including cloud storage.

RansomCare provides a layer of defense inside of a network even after the perimeter has been breached. When RansomCare detects a ransomware attack, an alert is raised instantly, and the software can automatically respond by shutting down and/or disconnecting the endpoint under attack (Windows, Mac, and Linux) so encryption stops. It can also alert system administration.

Members of OMNIA Partners can take advantage of Ricoh's national GPO contract

OMNIA Partners is the nation's largest, most experienced, and most trusted resource in group purchasing and supply chain management. OMNIA Partners unites industry-leading purchasing power and market-leading suppliers to deliver an extensive and diverse portfolio for members.

OMNIA®
PARTNERS

The Growing Threat from Ransomware

The news is often filled with stories of organizations, both large and small, that are victims of ransomware. These attacks impact business, education, healthcare, safety, and reputations, especially when personal information is compromised. Government warnings about ransomware are now common.

Cyber criminals are innovating new methods to defeat traditional signature-based methods of detection and to distribute the malware through other applications, phishing, USB drives, and even USB charging cables.

The Security of RansomCare

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. It does not matter which user or device triggered the attack, nor does it matter the source of the attack.

When RansomCare detects a ransomware attack, an alert is raised instantly and a response can be triggered to shut down and/or disconnect the endpoint, device and/or user under attack (Windows, Mac, and Linux) so encryption stops instantly. RansomCare also handles virtual environments.

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.

FREE Ransomware Assessment

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 in your environment to demonstrate how the solution responds to an outbreak. Ask your sales representative for more information.

For more information, please contact Travis Massman of Ricoh at 573-353-2559 or travis.massman@ricoh-usa.com

RICOH imagine. change.

www.ricoh-usa.com

www.omniapartners.com

OMNIA® PARTNERS

Ricoh USA, Inc., 300 Eagleview Blvd, Suite 200, Exton, PA 19341