RC
RansomCare

RansomCare (RC) is a Last Line of Defense that detects and stops active ransomware on file shares and servers by isolating any attacking users and devices.

Most organizations have already invested and deployed strong layers of security but still fear being vulnerable to ransomware. Cybercriminals have time and again proven to outsmart even the biggest organizations. Relying on existing preventative security is no longer enough. Cybercriminals use more sophisticated methods, outpacing traditional security vendors, and are capable of encrypting up to 10,000 files per minute, per attacking machine. RC focuses exclusively on the end game of ransomware instead of being another solution trying to recognize and prevent all malware. It is an agentless and proven containment system that monitors file- and cloud shares, isolating compromised users in seconds as soon as they start causing illegitimate encryption.

Existing security is consistently being bypassed by ransomware gangs.

The most efficient solution to the costliest cyber threat

RC does not depend on antiquated detection methods such as ransomware signatures, strains, patterns, or behavior. Instead, RC rapidly detects the purpose of the ransomware - the actual encryption. It does so without any network overhead or performance degradation. RC differentiates by monitoring file activity on file shares, application servers, and database servers. The RC detection technology operates using event-based file detection, with a raft of high-performance detection sensors inspecting the heuristics - regardless of the file

type or whether the file is renamed, modified, created, or deleted. RC detects the malicious encryption in seconds, whether on-premise or in your cloud. RC reacts by isolating any compromised user(s) or device(s) in seconds. RC can shut an offending machine down, disable the user in the cloud or Active Directory, revoke SMB permissions, disable VPN sessions, and much more.

Complements and enhances your existing cyber security investments

RC integrates with your existing security stack (ITAM, SIEM, EDR, NAC) via RESTful Web APIs and works in parallel with vendors such as Carbon Black, Varonis, McAfee, Symantec, SentinelOne, and Sophos - adding additional protection and enhancing the value of the existing cyber security tools. RC is fully scalable from SMEs to large-scale enterprises and is deployed to organizations globally. Companies of all sizes, from a few application- and database servers to enterprises with thousands of application- and database servers and hundreds of thousands of file shares and SharePoint sites, benefits from the additional protection.

RC delivers the ultimate ransomware defense for the budget

RC has repeatedly proven itself in the worst-case scenario, acting as the vital Last Line of Defense, mitigating the damage, disruption, and cost of active ransomware attacks, and protecting business-critical data on file shares and servers; RC detects when others fail to protect. Installation is done in a day and it is fully deployed remotely in weeks.

Next steps see it for yourself

🐂 **Experience BullWall's live demonstration**

🐂 **Learn about the ransomware assessment**

Concerned about ransomware? Contact BCyber to book a demonstration.