

STOP RANSOMWARE BEFORE IT STOPS YOU



NO ENDPOINT

AGENTLESS

Disclaimer: All trademarks are property of their respective owners. All company names used in this presentation are for identification purposes only. We make no warranties as to performance, merchantability, fitness for a particular purpose, or any other warranties whether expressed or implied. No oral or written communication from or information provided by BullWall or its resellers from this presentation shall create a warranty.







CommonSpirit Health Confirms It Was Hit By A Ransomware Attack



Jackson, Hillsdale County Schools, Canceled Due To Ransomware Attack



Lockbit Ransomware Claims Attack On Continental Automotive Giant



Costa Rica State of Emergency Declared After Ransomware Attacks



SHI Hit By 'Coordinated And Professional Malware Attack'



All trademarks are property of their respective owners. All company names used in this presentation are for identification purposes only.

PREVENTION-ONLY
STRATEGIES REQUIRE THAT...

You're **100%** effective,
↓100% of the time,
on **100%** of your attack surfaces,
against **100%** of threats.

The problem is you can't have 100% Prevention 100% of the time!



How do you:

- See which files are encrypted and where?
- Identify the attacker (patient zero)?
- Stop ongoing encryption?



External traffic



E-mail Scanner

Corporate Firewall



Web Gateway

Perimeter Protection

EDR, XDR, MDR

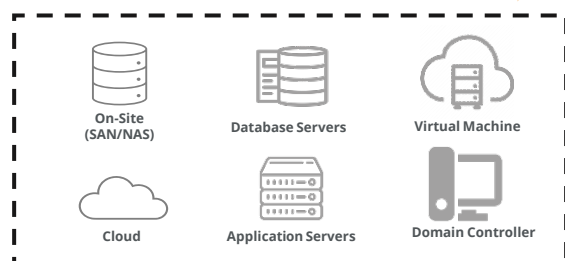


User/device isolated



First Line of Defense (Prevention-based)

Last Line of Defense



Data Storage & Critical IT Infrastructure



All trademarks are property of their respective owners. All company names used in this presentation are for identification purposes only.

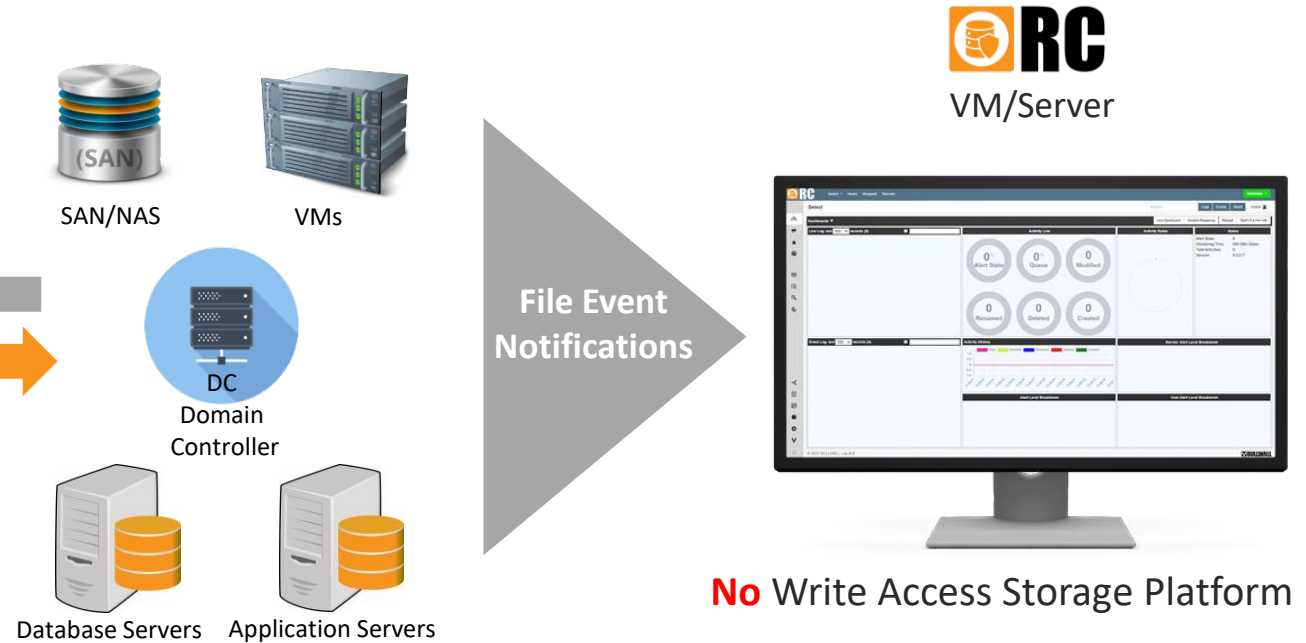


CLIENTS/ENDPOINTS



No Endpoint installation/Agentless
No Performance overhead

NETWORK IT INFRASTRUCTURE / DATACENTER



No Write Access Storage Platform

No Storage Platform installation
No Domain Controller installation
No Application- or Database Servers installation

RESULT = RANSOMCARE IS FAST AND EASY TO DEPLOY REMOTELY



FIRST LINE OF DEFENCE

Prevent malware attacks by looking for the virus itself initiated on endpoint devices.

LAST LINE OF DEFENCE

BullWall's RansomCare contains ransomware attacks by monitoring data created and modified by users or systems

Detect

Monitors user activity by leveraging 28 detection sensors and machine-learning capabilities.

Respond

Responds automatically to abnormal encryption events by isolating compromised user and alerting IT administration.

Recover

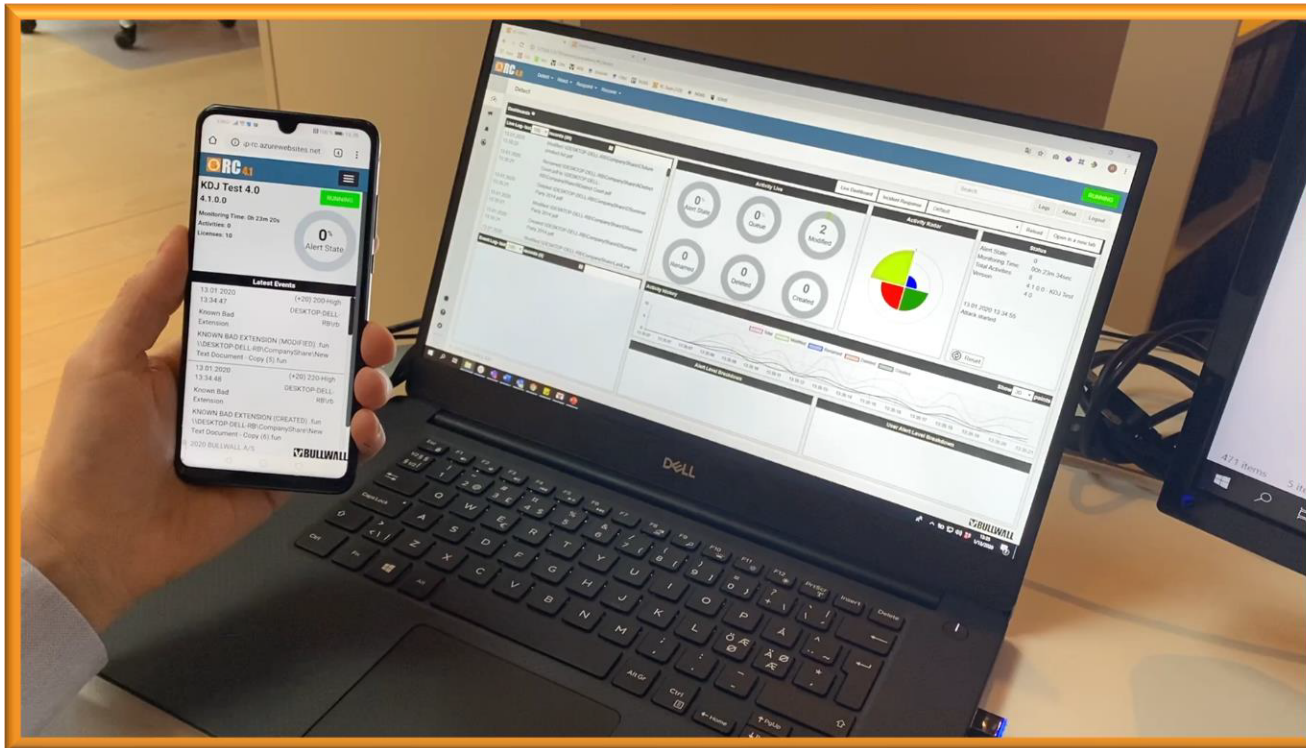
Expedited recovery by providing a list of compromised users and files to IT staff that can be integrated with back-up solutions.

Report

Provides a cyber incident report to internal leadership and external government agencies.



Built-in multi alerting services



- E-mail notification
- WhatsApp notification
- SMS alert
- Mobile "SOC"
- API to other system

RC can be integrated to any SIEM and NAC or other security solutions

2-way interface to RESTful API

	Initiate Cisco ISE isolation using the QuarantineByIp or QuarantineByMac method
	Monitoring of SOC team via integration to Splunk
	Large financial security provider in the Nordic, isolation via McAfee ePO
	Response and isolation using Symantec



DEMO OF AN ATTACK



Stop Ransomware Before It Stops You





UNDERSTAND THE CONSEQUENCES



Business Operations


NUMBER OF USERS ON THE NETWORK
How many users are in the Active Directory?
excl. service accounts



1,000 

Users in the AD


RANSOMWARE IMPACT
What percentage of employees will be impacted by a ransomware attack?



50 %

500 users offline


TECHNOLOGY DEPENDENT
How dependent are employees on technology to conduct normal operations?



80 %

Dependency on IT

AVERAGE EMPLOYEE COSTS
What is the average hourly cost per employee?
include wages, pension, and indirect costs such as office rental, etc.




50 \$

Total cost per employee


Business Recovery


According to Coveware, downtime is still the costliest aspect of a ransomware attack. In Q2 of 2022, the average firm experienced 24 days of downtime, a 3-day increase from 2020.



24 Days


OFFLINE SERVICES
How many hours will employees experience downtime while IT professionals restore online services following a ransomware attack?
One workday is equivalent to 8 hours.




192 

24 days = 192 hours

FILE RESTORATION
How many hours will it take for a single employee to recreate lost files that were unrecoverable from the data backup?




4 

COST OF DOWNTIME
You might not have the budget for additional protection. However, do you have the budget to cover the cost of recovering from a potentially devastating incident? The below calculation is just a loss of productivity, typically only 20-35% of the entire recovery cost.

\$3,920,000

Return on Investment

**Discounts are available for educational institutes, government agencies, and non-profit organizations.*

	One-year plan	Three-year plan	Five-year plan
<p>CYBER INSURANCE SAVINGS As a "Last Line of Defense" technology, RansomCare protects when others cyber solutions fail. Insurance companies often grant BullWall customers annual premium discounts since RansomCare controls ransomware outbreaks, much like a sprinkler system does a building fire.</p> <p>Input your annual premium and your expected savings.</p>  <div style="border: 1px solid black; padding: 5px; display: inline-block;">300,000 \$</div> <div style="border: 1px solid black; padding: 5px; display: inline-block;">10 %</div> Average savings 10-30%	<p>1 Year License Agreement:</p> <div style="border: 1px solid black; padding: 5px; display: inline-block;">42,663 \$</div> 3.6 \$ per user/mo. <p>Maximum Downtime Before investment is justified</p> <div style="border: 1px solid black; padding: 5px; display: inline-block;">128 Min.</div>	<p>3 Year License Agreement: Save 23% (255 Discount Days)</p> <div style="border: 1px solid black; padding: 5px; display: inline-block;">98,125 \$</div> 2.7 \$ per user/mo. <p>Maximum Downtime Before investment is justified</p> <div style="border: 1px solid black; padding: 5px; display: inline-block;">98 Min.</div>	<p>5 Year License Agreement: Save 38% (693 Discount Days)</p> <div style="border: 1px solid black; padding: 5px; display: inline-block;">132,255 \$</div> 2.2 \$ per user/mo. <p>Maximum Downtime Before investment is justified</p> <div style="border: 1px solid black; padding: 5px; display: inline-block;">79 Min.</div>
	<p>Years without Any Attack Before investment is not justified</p> <div style="border: 1px solid black; padding: 5px; display: inline-block;">92 Years</div>	<p>Years without Any Attack Before investment is not justified</p> <div style="border: 1px solid black; padding: 5px; display: inline-block;">120 Years</div>	<p>Years without Any Attack Before investment is not justified</p> <div style="border: 1px solid black; padding: 5px; display: inline-block;">148 Years</div>
<p>Premium savings</p> <div style="border: 1px solid black; padding: 5px; display: inline-block;">30,000 \$</div>	<p>Cost after Reduction License cost minus insurance savings</p> <div style="border: 1px solid black; padding: 5px; display: inline-block;">12,663 \$</div>	<p>Cost after Reduction License cost minus 3-year insurance savings</p> <div style="border: 1px solid black; padding: 5px; display: inline-block;">8,125 \$</div>	<p>Cost after Reduction License cost minus 5-year insurance savings</p> <div style="border: 1px solid black; padding: 5px; display: inline-block;">-17,745 \$</div>

Step 1

You will receive a prerequisites document that requires preparation before the online session



30 minutes



Follow prerequisites



Setup test share

Step 2

Using our simulator, we run several simulations with ransomware behavior



How does your network react?

We simulate that your endpoint protection is circumvented. What is the next layer to detect the malware?



Experience RC in your environment

We re-run the simulations, this time with RC set to monitor the test file share.



Will your existing security react?

We re-run the simulations, this time with your existing security solution running to see if they stop the encryption and ransomware behavior.

Step 3

Since the development of the assessment tool, over 94% found the two-hour session to be very enlightening



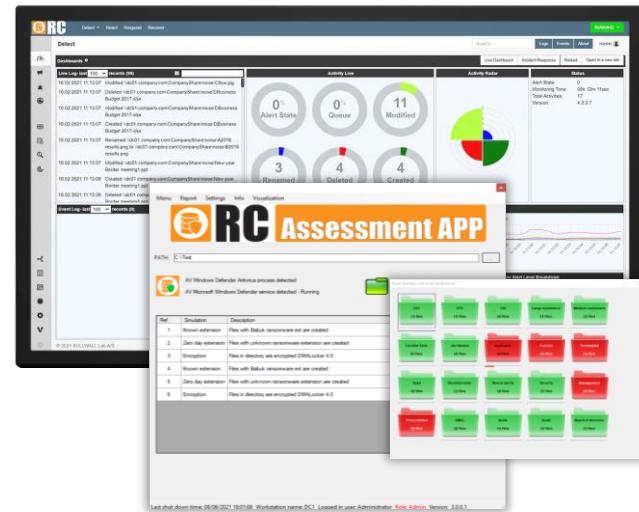
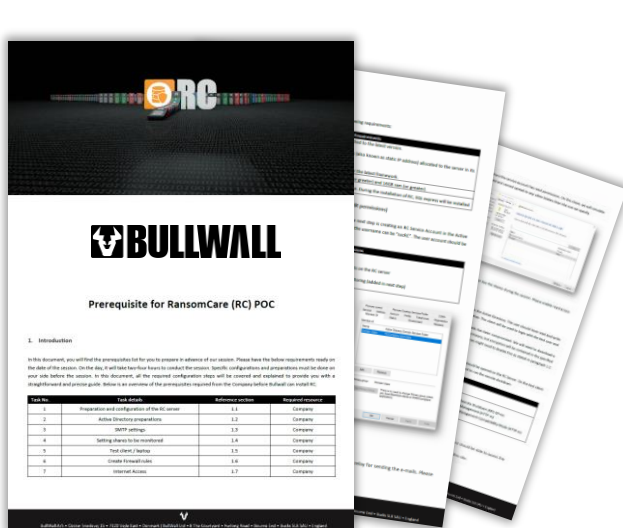
Global assessments



Reporting available



Understand your resilience to an encryption outbreak



Task No.	Task description	Reference version	Required version
1	Preparation and configuration of the RC server	2.1	Compatible
2	Active Directory permissions	2.2	Compatible
3	SMTP settings	2.3	Compatible
4	Setting shares to be monitored	2.4	Compatible
5	Test share creation	2.5	Compatible
6	Create Firewall rules	2.6	Compatible
7	Internet Access	2.7	Compatible

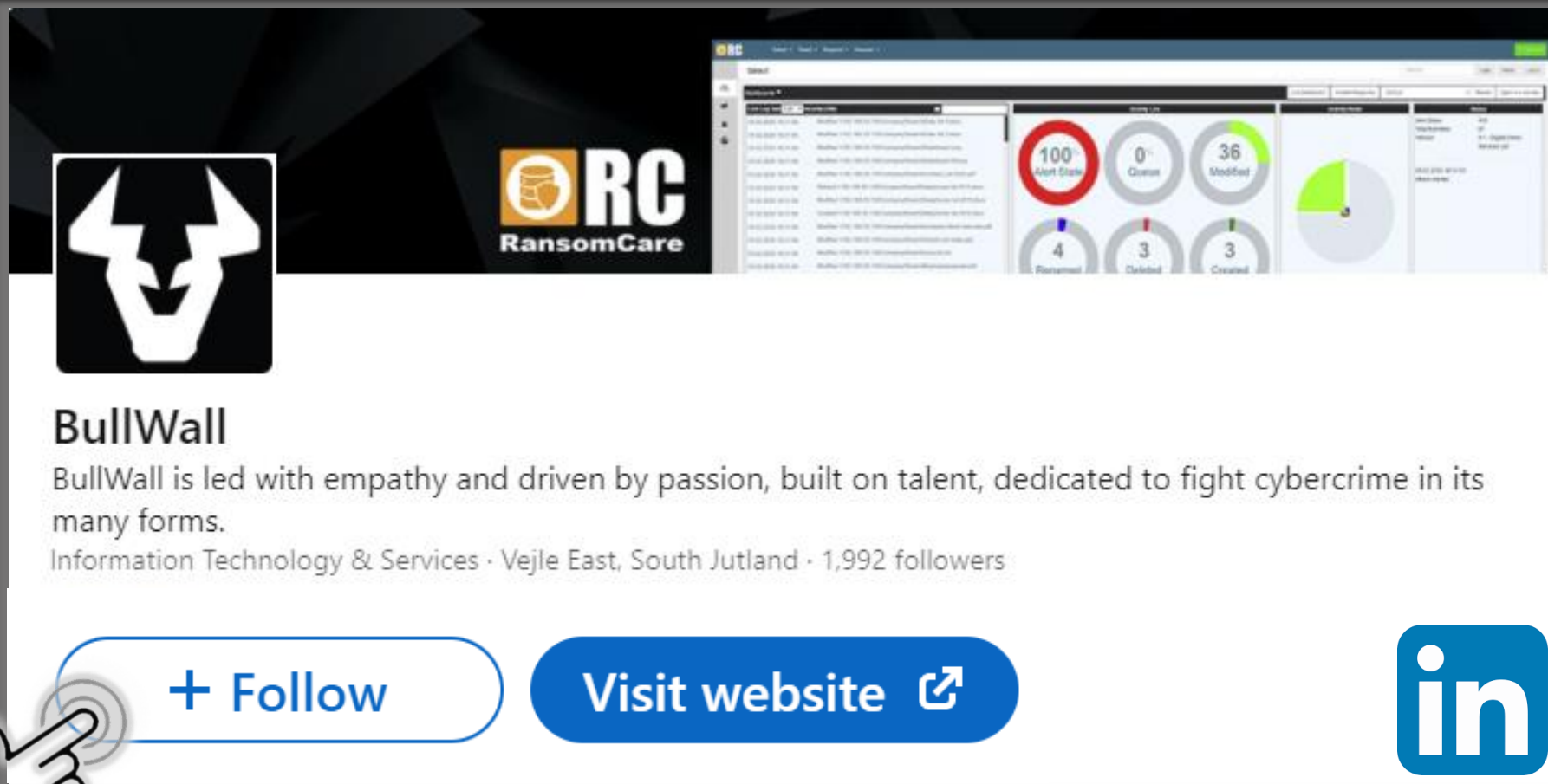
Thank you for your time and attention!



Disclaimer: All trademarks are property of their respective owners. All company names used in this presentation are for identification purposes only. We make no warranties as to performance, merchantability, fitness for a particular purpose, or any other warranties whether expressed or implied. No oral or written communication from or information provided by BullWall or its resellers from this presentation shall create a warranty.

Thank you for your time and attention!

To keep up to date with Ransomware News and BullWall Updates... Follow BullWall on LinkedIn!



BullWall
BullWall is led with empathy and driven by passion, built on talent, dedicated to fight cybercrime in its many forms.
Information Technology & Services · Vejle East, South Jutland · 1,992 followers

[+ Follow](#) [Visit website](#)

