BULLWALL

CUSTOMER STORY

BULLWALL HELPS MANUFACTURING COMPANY SPEED UP RECOVERY WHILE SAFEGUARDING AGAINST NEW THREATS

Industry

Manufacturing

Location

Canada

Users

1,200

SECURITY STACK

CISCO

Symantec. by Broadcom Software

FILESHARE INFRASTRUCTURE

Cloud

OVERVIEW

After a ransomware attack caused more than a month of downtime in 2022, a Canadian raw material manufacturing company knew it needed a better solution to mitigate future threats. The company turned to BullWall for help. During installation, BullWall's sensors detected numerous bad extensions remaining in their environment from the previous attack. This reassured company leaders that BullWall's solution could quickly and accurately pinpoint threats in their environment and help the team recover faster in the future.

THE LINGERING THREAT OF A RANSOMWARE ATTACK

Ransomware attacks have increased by 232% since 2019, leaving organizations across every industry scrambling to protect themselves.[1] But many companies are discovering that the ransomware threat can linger beyond the initial attack. In fact, ransomware victims are 80% more likely to experience another attack if the company does not correctly restore and strengthen security protocols.

In early 2022, a large Canadian manufacturing company learned this lesson the hard way after being hit by Phantom ransomware.

The ransomware strain circumvented the company's existing security solutions, causing over a month of downtime as IT administrators worked around the clock to restore their servers and data. Not only did the extended downtime impact operations, but the team struggled to identify all corrupted files and devices—a manual, error-prone process—leaving the company exposed.

232%

Increase in ransomware attacks since 2019

80%

Ransomware victims that experience **another attack**

75%

Organizations that were unable to recover data from **backup**

COSTLY DOWNTIME AND AN OVERBURDENED IT TEAM

After the company's significant impact from just this attack, they wanted to understand if they were vulnerable to others. To do so, the company conducted a BullWall Ransomware Assessment to evaluate if they were vulnerabilities to additional ransomware strains. This controlled assessment uses real ransomware variants to demonstrate how an organization's security infrastructure responds to an active attack in its environment.

[1] SonicWall, "2022 SonicWall Cyber Threat Report"

BullWall tested three variants in the company's environment and confirmed they needed an additional layer of security to contain ransomware attacks and to support their continued recovery. BullWall then began working with the company to deploy its ransomware solution.

While administrators now understood they needed another line of defense against ransomware strains, they were still recovering from the Phantom attack. They had limited time and resources to invest in managing a new security solution. They needed a solution that could be easily and rapidly deployed with minimal burden on their already over-extended IT department.

For them, the choice was clear.

OLD THREATS UNCOVERED, NEW THREATS CONTAINED

BullWall takes the burden off security teams every step of the way. As an agentless solution, it requires minimal involvement from the IT team during the installation. This allowed the IT team to focus on recovery while enhancing their security infrastructure against another attack.

Even though BullWall's ransomware solution is designed to contain active attacks, it also helps with threat hunting by identifying corrupted files rapidly and reliably, helping teams recover even faster. And the manufacturing company benefitted from this capability right away.

During the installation, a BullWall security engineer noticed an abnormal number of alerts from the solution's detection sensors. Instead of an active attack, the sensors detected bad extensions left over from the company's previous attack. This enabled the IT team to quickly identify corrupted files they had missed, saving valuable time, reducing the manual burden, and accelerating recovery.

Although the alerts were triggered based on a previous attack, BullWall's solution gave the IT Director greater peace of mind that the team is better prepared to mitigate and recover from future ransomware attacks.

ABOUT BULLWALL

BullWall is a cybersecurity solution provider with a dedicated focus on protecting data and critical IT infrastructure during active ransomware attacks. We are able to contain both known and zero-day ransomware variants in seconds, preventing both data encryption and exfiltration.

BullWall is your last line of defense for active attacks.

Learn more at www.bullwall.com.

BULLWALL

Version 2023.04