BULLWALL

CUSTOMER STORY

FROM RANSOMWARE AND BEYOND: BULLWALL HELPS U.K. GOVERNMENT AGENCY PREVENT SECURITY BREACH

Industry
Government

Location
United Kingdom

Users
7,500

FILESHARE INFRASTRUCTURE

Cloud

OVERVIEW

Following years of rebuilding public trust after a security breach in 2009, cybersecurity is an increasingly high priority for one U.K. government agency. With cyber threats against government organizations on the rise, the agency was looking for a solution that could deliver greater visibility into its environment and reliable ransomware protection for a newly remote workforce. BullWall's solution not only contains active ransomware attacks, but it provides real-time visibility, enabling the agency to identify non-ransomware threats wherever they occur in their environment.

GROWING CYBER THREATS PUT U.K. GOVERNMENT AGENCIES AT RISK

In 2022, U.K. organizations experienced an average of 788 weekly cyber attacks—a 77% increase from 2021—spurring many to redouble their cybersecurity efforts.[1]

This includes one U.K. government agency that is still repairing its public reputation more than a decade after a security breach back in 2009 when two laptops were stolen from the local town hall. The laptops, which contained sensitive personally identifiable information (PII), including data on 1,754 employees at local schools. The breach resulted in public outcry and a costly lawsuit, forcing the organization to prioritize data security.

However, despite the agency's ongoing efforts to improve security over the years, the recent rise in ransomware attacks—especially against other government agencies—has brought the issue to the forefront once again.

788
Avergage **weekly cyber attacks in 2022**

77%
Increase from 2021- Thus redoubling efforts

1,754
Employee data at local schools

LEADERS UNDER INCREASED PRESSURE

In 2021, one agency leader warned in 2021 that the organization's cyber security systems had experienced thousands of attempts to breach the systems. This is especially concerning in the UK, where organizations took an average of 181 days to identify that a breach had occurred and another 75 days to contain the incident.[2]

As a result, the agency's leaders were increasingly concerned with protecting residents' data and ensuring services remain online so officers could carry out their roles. But this proved an

[1] ITPro.co.uk, "Cyber attacks on UK organisations surged 77% in 2022, new research finds"

[2] Comparitech, "UK cyber security and cyber crime statistics (2023)"

especially challenging task since the agency transitioned to a remote workforce and cloud-based solutions after the pandemic, leaving a broader attack surface to protect. And, despite experiencing multiple security breach attempts, the agency had never tested its infrastructure with live ransomware strains to identify its vulnerabilities.

The agency needed a solution that addressed the increase in attacks and assisted with user visibility within their IT network to prevent security breaches. Amidst these growing concerns, the organization leaned on BullWall, the global leader in ransomware containment, for support.

BullWall conducted its Ransomware Assessment with three real-life ransomware strains to evaluate the agency's vulnerabilities to security breaches. As usual, the test confirmed they were vulnerable to these ransomware variants and needed an additional layer to contain active ransomware attacks and speed recovery.

Armed with this new information, the agency immediately implemented BullWall as a last line of defense to protect what matters most—their data.

GREATER VISIBILITY UNCOVERS MULTIPLE THREATS

BullWall addresses the agency's top security breach concerns, providing real-time visibility to their IT team and automatically containing malicious encyptions from bad actors.

"We cannot take our eyes off the ball, and RansomCare has given us the additional eyes to help tackle this type of activity," shared the IT manager.

> *We cannot take our eyes off the ball, and RansomCare has given us the additional eyes to help tackle this type of activity.*

But BullWall's solution provides security and peace of mind beyond ransomware threats. The agency experienced this benefit firsthand when a remote employee downloaded an unauthorized game on his company laptop, which began to encrypt and exfiltrate data from the IT network. Although the threat was not ransomware, BullWall detected this malicious activity, instantly isolated the user to prevent a further security breach, and alerted the IT team. As a result, the agency was able to take swift action to identify the employee and investigate the incident.

"Thankfully, it wasn't a ransomware attack this time, but it was user activity that shouldn't be happening," the agency IT manager explained. "As a result, the employee is going through discipline action to prevent this type of activity from happening on the network again."

With BullWall, the agency has greater visibility into its network to prevent further data breaches–from internal or external sources–and will be prepared for an inevitable security breach.

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.

Version 2 | 二版
www.version-2.com
Hong Kong | Taiwan | Singapore | Macau | Mainland China

Version 2023.04