BULLWALL

CUSTOMER STORY

BULLWALL SAVES MAJOR EUROPEAN FINANCE COMPANY $35.8 MILLION WITH RANSOMCARE

Industry
Finance

Location
Europe

Users
7,000

SECURITY TOOLS

Genetec
McAfee
mimecast

FILESHARE INFRASTRUCTURE

Cloud

On Premises

SUMMARY

A leading European financial firm serving over 5 million customers in the private, commercial, and corporate markets needed a cybersecurity solution to mitigate the rising threat of ransomware attacks. After their network of security solutions failed to protect them—costing critical downtime and millions of dollars—they turned to BullWall. Leveraging BullWall RansomCare, the finance company quickly identified and neutralized security threats with minimal disruption to their operations. Over 5 years, the company has saved over $35 million using BullWall's solution.

AN INDUSTRY HELD HOSTAGE

Ransomware is a growing threat to organizations around the world. The financial service industry has been hit particularly hard with a 35% rise in attacks quarter-over-quarter in 2022, including a 13% increase in ransomware attacks on insurers. Finance companies handle a significant amount of personally identifiable information (PII), making them ideal targets for ransomware attacks.[1]

Seeking to protect itself against these growing threats, one leading European financial service firm adopted a collection of preventative solutions. It implemented a robust security stack of Mimecast, Cisco, Symantec, and McAfee and hired a 24-hour IT Security Company to monitor their network environment for malicious cybercriminal activity manually. But when a ransomware attack occurred, the finance company was left scrambling to mitigate the damage.

4,000
Impacted Employees

9
Downtime Days

429K
Encrypted Files

THE HIGH COST OF INADEQUATE PROTECTION

Despite the company's extensive security stack, ransomware could propagate undetected, and an active attack was discovered purely by coincidence. Security analysts were monitoring fileshare activity to review the number of active employees on a business application. During this routine review, the analysts inadvertently noticed malicious encryption activity taking place within the network.

Over the next four hours, **429,000** files were encrypted as IT personnel frantically rushed to unplug IT equipment to prevent further infrastructure damage. The breach caused 9 days of operational downtime and cost the company an estimated **$8 million**.

[1] PropertyCasualty360.com "Most industries seeing relief from ransomware, but insurance isn't one," May 2022

Seeing that their current security stack had failed to identify or prevent the ransomware attack, the company's CISO knew they needed another layer to their security stack.

The company became aware of an innovative cybersecurity company BullWall, which developed RansomCare. Unlike other solutions, which focus on ransomware prevention, BullWall detects and contains active ransomware attacks by monitoring the activity on file shares, cloud data storage, application servers, and database servers. RansomCare does not depend on outdated detection methods such as ransomware signatures, strains, patterns, or behavior. Instead, RansomCare rapidly detects both known and unknown strains of ransomware by identifying malicious file activity. It does so without any network overhead or performance degradation. Later that year, BullWall was put to the test.

3

Impacted Employees

0

Downtime Days

101

Encrypted Files

MONEY SAVED. TRUST EARNED.

During a routine update, the email compromise tools were offline for 19 minutes. In that short time, three employees opened malicious email attachments that began to encrypt data rapidly.

Within seconds, BullWall's solution automatically isolated the three users by disconnecting them from Active Directory to prevent widespread damage. BullWall then alerted IT personnel, providing a list of all compromised users, devices, and data. This enabled the team to focus on restoring the network instead of manually investigating the incident, slashing their recovery time. Thanks to BullWall's solution, the threat was contained before the IT Security Monitoring Provider had even detected the malicious activity.

As a result, all data and endpoints were fully restored and operational within 24 hours.

On average, companies hit with ransomware experience 24 days of operational downtime, costing $4.62M to recover. Since its installation, BullWall has saved the company an estimated **$35.8 million**, reduced downtime from days to hours, and given them peace of mind that their data is secure across the organization.

$35.8M

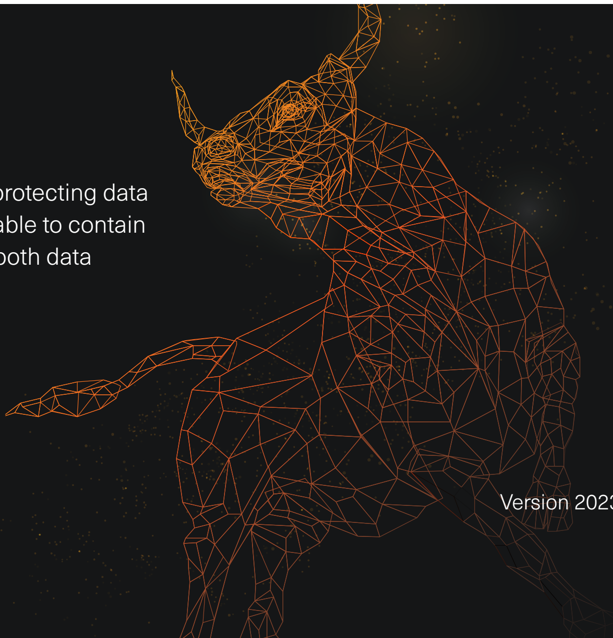
TOTAL SAVINGS FROM RANSOMCARE

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