



BULLWALL FOR FINANCE

Financial institutions hold vast amounts of sensitive customer information which makes them a prime target for ransomware attacks.



THE CONSEQUENCES OF ATTACKS ON BANKS ARE LONG-LASTING, PUTTING BRAND REPUTATION AND CUSTOMER LOYALTY AT RISK.

With limited resources and aging infrastructure, financial institutions are forced to prioritize budget and time on immediate threats, making rapid ransomware containment a necessity to minimize downtime and protect operations.



WHY BULLWALL?

BullWall automatically prevents and contains cyber threats, ensuring financial institutions maintain operational continuity, protect sensitive customer data, and minimize disruptions to services during an attack.

65%

of financial services organizations experienced a ransomware attack in 2024

90%

of financial services organizations had **cybercriminals attempt to compromise their backups**

The State of Ransomware in Financial Services 2024, Sophos



Cybercriminals have become too advanced for banks to rely solely on prevention. We need strong containment strategies to limit damage and keep our services running, ensuring resilience even if an attack breaks through.

MARK JAMES
CIO, Citizens First Bank





HOW FINANCE BECOMES A RANSOMWARE TARGET



 **TARGETING BACKUPS**

90%
of ransomware attacks targeted financial services organizations' backups in 2024, exploiting them to disrupt recovery efforts, forcing organizations to pay ransom.



 **LATERAL MOVEMENT**

30%
of ransomware attacks in 2024 were caused by compromised credentials, which allow cybercriminals to move laterally across the network, bypass security measures, and deploy ransomware.



 **EXPLOITED VULNERABILITIES**

27%
of successful attacks used exploited vulnerabilities in legacy IT systems and third-party tools, taking advantage of delays in patching to gain entry and deploy ransomware.

THE IMPACT

In recent years, ransomware attacks have severely impacted financial institutions, with over 395 confirmed attacks compromising the records of at least 84.6 million customers.



FINANCIAL LOCKDOWN AND ERRORS

Operating systems and transaction data can be locked, preventing customers from accessing their accounts, payment delays and even errors in financial accounting.



CUSTOMER IDENTITY THEFT

Cybercriminals sell stolen customer data on the dark web, exposing victims to identity theft, fraud, and blackmail, leaving customers feeling neglected and vulnerable to long-term financial damage.



FINANCIAL AND OPERATIONAL IMPACT

Ransomware attacks can cripple financial organizations for weeks, with recovery costs averaging \$2.58 million in 2024. These costs include ransom payments, IT recovery expenses, legal fees, fines from regulatory bodies such as the GDPR, DORA and PCI DSS, and the loss of business due to operational downtime. Financial institutions that swiftly contain and mitigate an attack can significantly lower recovery costs and minimize prolonged disruptions, reducing long-term financial and reputational damage.



WHAT IS RANSOMWARE RESILIENCE?

Ransomware resilience is the ability to prevent, contain, and respond to ransomware attacks, minimizing damage and ensuring rapid recovery of data and operations to maintain business continuity.



PREVENTION

Reduce the risk of disruptions to operations, which can be costly and damaging to productivity.



CONTAINMENT

Minimize the impact to business operations when ransomware gets through, and significantly reduce recovery efforts.



RECOVERY

Resilient organizations recover quickly to limit operational downtime and return stronger.

BE RANSOMWARE READY... WITH BULLWALL

BullWall's unique approach to ransomware provides server-based protection without an endpoint agent to secure critical IT infrastructure and maintain operational continuity across all stages of an attack—before, during, and after.

Cybercriminals often target backups to disrupt recovery efforts, customer services and force financial institutions to pay ransom.



BullWall is the only solution that immediately contains an active attack, preventing ransomware from reaching and encrypting backup systems, ensuring business continuity without the need for ransom payments.

Compromised credentials enable cybercriminals to move laterally across a network, exfiltrate data and disable security tools.



BullWall addresses urgent gaps left by traditional security solutions, preventing compromised credentials from being exploited, revealing adversaries on the network, and preventing cybercriminals from disabling security solutions.

Legacy IT equipment and third-party tools are often vulnerable to exploitation by ransomware, providing attackers with an entry point to deploy malicious payloads.



BullWall protects all data and critical IT infrastructure, ensuring that no matter the entry point ransomware is contained before it can disrupt critical data and systems.

THINK YOU'RE RANSOMWARE RESILIENT? **FIND OUT FOR SURE.**

BOOK ASSESSMENT



BULLWALL

**RANSOMWARE RESILIENCE
FOR CRITICAL IT INFRASTRUCTURE**

