Pillar Technology
PARTNERS

INCIDENT RESPONSE CASE STUDY

From Incident Chaos to Smart Security:
A Mid-Market Organization's Journey to Resilience

Incident Summary

When a mid-sized organization faced a cybersecurity breach, their IT leader was overwhelmed, managing both IT operations and security with limited resources. With no clear incident response plan and a constrained budget, they needed immediate support. Pillar's rapid response team not only contained the threat but also implemented a long-term security solution that fit their financial and operational constraints.

The Challenge

The call came in on Pillar's Incident Response Line—an IT leader in distress, facing an active cybersecurity breach. Like many organizations of their size, this client had a lean IT team responsible for both infrastructure and security. The lack of dedicated security personnel made them vulnerable, and the attack exposed multiple gaps in their environment. With operations spanning five remote sites, they needed immediate containment and a scalable security solution that wouldn't strain their limited budget.

PILLAR'S RESOLUTION

The Response

Pillar's team quickly mobilized, deploying technicians to all five remote locations to contain the threat and assess the extent of the breach. Our forensic investigation revealed the attacker's point of entry, along with several other vulnerabilities that required urgent attention.

Understanding the client's financial constraints, we took a pragmatic approach. We categorized the security gaps based on risk level and impact, enabling the IT leader to present a data-driven case to executive leadership. The conversation shifted from a technical discussion to a business imperative —demonstrating the financial and operational impact of cybersecurity threats.

The Solution

Pillar recommended its modular security solution, PTechXMS, designed specifically for mid-market organizations. This fully managed security service would alleviate the burden on the IT team while delivering enterprise-grade protection. Given the budget limitations, we prioritized implementation in phases:

1

Managed Detection & Response (MDR)

Immediate deployment to monitor and neurtralize future threats.

2

Firewall Management

Ensuring perimeter security and threat prevention.

3

Security Information & Event Management (SIEM)

Centralizing security data to provide visibility and rapid response capabilities.

By implementing the most critical components first, the client was able to secure funding incrementally while strengthening their security posture.

PILLAR'S REMEDIATION

The Results

With Pillar as their cybersecurity partner, the organization transformed its security approach from reactive to proactive. The IT leader regained control of their operations, knowing that a dedicated team was monitoring their environment 24/7. Nights and weekends were no longer consumed by security concerns, and executive leadership had confidence that their business was protected.

Today, the client not only benefits from managed security services but also ongoing CISO-level guidance, ensuring their security strategy evolves with emerging threats. Pillar's partnership extends beyond protection—it provides peace of mind and a clear roadmap to resilience.

The Conclusion

This case study exemplifies how a mid-sized organization can navigate a cybersecurity crisis and emerge stronger with the right strategy and support. Pillar's mission-driven approach ensures that even organizations with constrained budgets can achieve robust security without compromising their business objectives.

First Defense

Financial Loss: The breach posed a direct financial risk, with the potential for customer data exposure, unauthorized transactions, and regulatory penalties. Our immediate action focused on securing critical financial systems and ensuring no further unauthorized access occurred.

Minimizing Downtime: To contain the threat, affected systems were isolated, and non-essential network connections were severed. This step helped prevent further spread while enabling safe remediation without prolonged disruption to business operations.

Stopping Infection Spread: Our forensic analysis pinpointed the attack's origin—an insecure system configuration that exposed internal assets to external threats. We swiftly removed the compromised access points, patched vulnerabilities, and implemented stricter security controls to prevent reinfection.

678-304-9099
info@ptechcyber.com
www.ptechcyber.com