



ARMOR XDR+SOC USE CASE



Treatment Center Rapid Growth Risks

Public cloud limitations with minimal response ability
disrupt compliance security posture



INTRODUCTION

A US-based company with over 200 retail pain management treatment centers is growing rapidly and is concerned about maintaining effective security and HIPAA compliance.

Since their data is in the AWS public cloud, they are concerned about meeting requirements for the medical insurance industry and they also want to pursue HITRUST certification.

- **Industry:** Healthcare
- **Company Size:** 1000+
- **Certifications:** HIPAA
- **Technologies:** AWS

To scale their business, they are designing applications moving from IaaS to PaaS with microservices and containers. Their solutions generate log and data telemetry that require security inspection.

With no SOC team to manage security, limited IT, and the limitations of the cloud shared responsibility model they are anxious to find a solution.

They need a partner with a unified platform that can provide them with secured data not only at the corporate level but also at the business unit level.

HOW ARMOR DETECTS AND RESPONDS

The **Armor XDR platform** provides visibility into all their infrastructure in a single view while preserving the ability to drill down to individual business units.

Armor directly supports compliance efforts for commonly implemented risk and security frameworks, including ISO-27001, NIST, PCI and HITRUST. Armor also shares or inherits responsibility for a broad array of common controls:

- Anti-malware
- Technical vulnerabilities
- Threat detection
- Reporting information security events
- Responses to information security incidents

Armor's solutions provide the cost and flexibility of a cloud-native approach that's based on open standards and industry-accepted best practices

- **Armor XDR+SOC**
Correlate data from your cloud, SaaS, OT, and workplace environments to detect and eliminate threats.
- **Armor GRC|P**
Simplify compliance and manage your global enterprise risk posture with a modern, full-service risk management solution.



Armor XDR+SOC enables the customer's GRC team to have a comprehensive view into company risk posture, significantly reducing the likelihood of a security incident and serves as a critical component of their incident response plan. This results in substantially improved risk resilience and intrusion tolerance in the event of a severe security incident.

The **Armor SOC team** analyzes all the telemetry from their security tools, creates incident notifications, runs automated remediation if applicable, and remediates threat actors and vulnerabilities within their infrastructure, enabling them to prevent breaches and stay HIPAA compliant.

- Single platform to reduce complexity and increase visibility to investigate threats
- Performance and cost savings with cloud-enabled security
- Remediation by proven, effective team of analysts, engineers, and forensics experts

MAINTAIN COMPLIANCE

As a result, the company is able to mitigate risks from threat actors and respond in a timely fashion in the event an issue is found as well as:

- Maintain their HIPAA compliance framework consistently
- Simplify their audit process
- Provide reporting necessary for the audit



What does Armor do to help protect organizations?

At Armor, we are laser-focused on creating desirable security outcomes.

Tell us which conditions require specific actions and Armor will design the security script to execute, so many threats will be mitigated automatically.

Integrate our SOC with your security team

Enacting a disaster recovery (DR) plan

Offer GRC Services to help you maintain compliance

Enacting an incident response plan (IRP)

Be your trusted partner throughout the lifecycle of a cyber threat

Conduct guided IRP tests regularly

ARMOR XDR+SOC

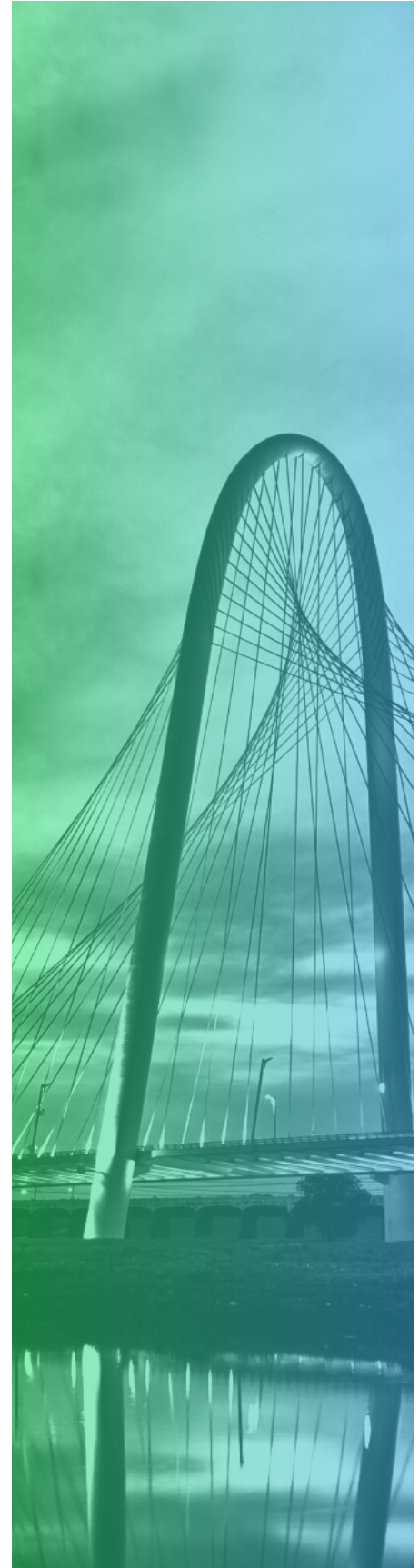
Armor's XDR+SOC solution combines cloud-native detection and response capabilities with our 24/7 team of cybersecurity experts utilizing our comprehensive, threat hunting and alerting library to deliver critical security outcomes.

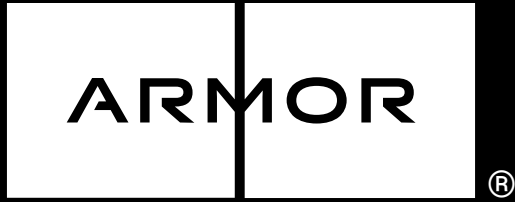
Available on-demand and delivered in native ways that supercharge your security program to improve your risk and compliance posture. Our Security Operations Center adds a layer of cybersecurity expertise to respond to threats quickly and thoroughly to inform and guide remediation efforts.



ABOUT ARMOR DEFENSE

Armor is a global leader in cloud-native managed detection and response. As a trusted partner to more than 1,500 firms in over 40 countries, Armor offers cybersecurity and compliance consulting, professional services, and managed services. Armor's industry-leading experts leverage non-proprietary frameworks and a 24/7/365 SOC to help organizations tackle the complexities of cybersecurity and compliance at a cloud-scale.



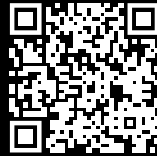


WWW.ARMOR.COM (US) +1 877 262 3473 (UK) +44 800 500 3167

©2023 Armor Defense Inc. All rights reserved.



CONTACT US
TO LEARN MORE



REQUEST A FREE
CYBER HEALTH CHECK