ARMOR XDR+SOC USE CASE

Saas Provider Cloud Migration Exposure

Maintaining compliance when moving from private to public cloud

INTRODUCTION

A US-based medical SaaS company offering a single point of care mobility interface solution for chronic disease management, transition care, remote home health care, lab integration, physician billing and telemedicine. They are concerned about maintaining effective security and HIPAA compliance while using AWS public cloud.

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

The customer needs to leverage the AWS Aurora solution to enhance performance of critical databases and to scale their business. They need to move from VPC to AWS environment quickly. Security and HIPAA compliance requirements must be considered during this process.

They have a variety of solutions that generate log and data telemetry which require security inspection. Cloud-native sources like AWS GuardDuty and CloudTrail are important components to be evaluated.

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.

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.

Armor XDR+SOC provides protection against unauthorized access to PHI by monitoring telemetry data for every access request. They can ensure that data is only accessible from managed devices or known IP addresses.

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.

In addition, **Armor's XDR+SOC** can inform on any violations of HIPAA policies or procedures, and it can prevent access attempts which do not conform to them.

Armor's GRC|P services can assist with the review of existing policies or procedures and ensure they are documented in compliance with HIPAA standards implementation specifications. We can also help tune the XDR+SOC deployment to identify and automatically block problematic activity to significantly reduce the likelihood of a breach.

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.

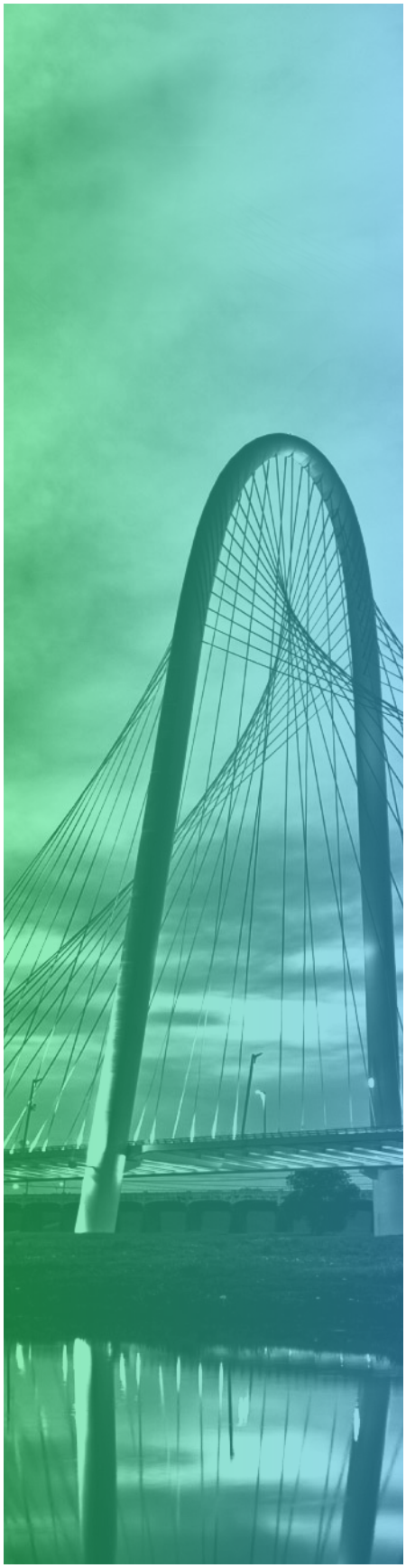
Tell us which conditions require specific actions and Armor will design the security script to execute, so many threats will be mitigated automatically.

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

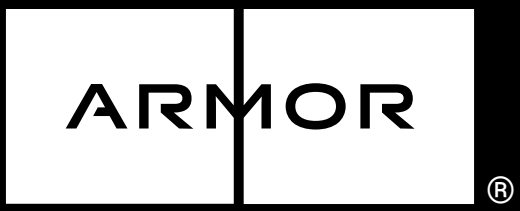
Armor's XDR+SOC solution combines cloud-native detection and response capabilities with our 24/7 team of cybersecurity experts utilizing our comprehensive, threat hunting and alerting library to deliver critical security outcomes.

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

CONTACT US
TO LEARN MORE

REQUEST A FREE
CYBER HEALTH CHECK