P1 PROTECT

Ransomware Response For Healthcare

The security engineers at a top ten hospital in California recognized that ransomware was not only on the rise, but that healthcare organizations were prime targets for threat actors. They poured hours into fortifying their data protection environment. Lives were at stake, and they knew that if they were attacked, they had to be ready to respond.

The challenge quickly became managing data protection alongside the rest of their initiatives. Resources are finite, and every technology organization has to make choices. Instead of deprioritizing security and defense, they chose **P1 Protect**, a comprehensive Data Protection as a Service (DPaaS) offering from the experts at P1 Technologies.

> "Know your enemy and know yourself, and you can fight a hundred battles without disaster."
>
> **Sun Tzu,** *The Art of War*

An Attack Blueprint

We know that threat actors come in all shapes and sizes and leverage a variety of platforms and utilities to exploit different attack vectors. However, most attacks follow a standard procedure:

1. PENETRATE THE NETWORK
2. EXPLOIT A CENTRAL AUTHENTICATION SYSTEM
3. MOVE LATERALLY
4. INFILTRATE AND CONTROL SYSTEMS/DATA
5. SEEK AND DESTROY BACKUPS

This attack blueprint was used to shape the architecture and design of P1 Protect, and the primary reason it was **deployed outside of the hospital's authentication sphere.** If an attacker were to attain privileged access credentials, those credentials would be useless in an attempt to access data protection copies.

P1 Technologies
Boots in the Cloud

A Layered Security Approach

Here's what else we know about our enemy: they're talented, motivated, resourceful, and relentless. One line of defense is simply not enough. Instead, the architects at P1 worked with the hospital to employ a layered security approach. A separate authentication sphere was just the first layer of defense. Air-gapping data protection copies in an isolated environment was the next step.

Air-Gapped Protection

Public cloud was the obvious choice to build an isolated environment outside the hospital's. A landing zone could be deployed with ease using Infrastructure as Code (IaC), but more importantly, that same code could be used to detect and prevent drift from the hardened security standard used during initialization. Many environments start with a strong security posture, but configuration changes made over time can stray from security standards and become a source of vulnerability. IaC state and an advanced detection system, tightly integrated with AWS GuardDuty and CloudTrail, would allow P1 Protect Ops to identify and remediate configuration or activity that might compromise the hospital's security posture.

Immutable Storage Target

If you truly know your enemy, you know it's naive to believe that even with all these defense mechanisms in place, any environment is impregnable. This is where immutability comes in. The best way to prevent anyone, both malicious and unaware actors, from tampering with data is quite simple: after a protected copy is written, disable subsequent writes. This feature, commonly referred to as WORM (write once, read many), would be used to write at least one protected copy for all of the hospital's critical data.

However, **not all immutability is created equal**. Immutability at the data protection platform layer is nice, but if the underlying storage subsystem is compromised, it's useless. Immutability at the storage layer is better, but again, if that storage system is compromised, although data can't be encrypted or destroyed, the storage system itself could be bricked or rendered inoperable. Immutability or not, once a storage system is inoperable, recovery will be impossible.

If we game this out and an attacker has made it this far in a quest for backups, the goal isn't to get the data—that's already happened. It's simply to prevent recovery and improve their leverage. With this in mind, the architects at P1 chose to employ AWS S3 object locking for immutability. If an attacker is trying to prevent recovery, taking a system down does the job. Downing a self-managed storage system is a challenge but not insurmountable, especially if central authentication has already been compromised. Downing the S3 storage service from AWS is a significantly taller task.

P1 didn't select AWS S3 for security alone. The Glacier Instant Retrieval storage class provides an **optimal balance of cost and recovery speed for data protection.** It's also as durable as a storage system gets. All told, it serves as an ideal storage backend for the hospital's last line of defense.

Securing the Process

With a well-architected data protection system in place, we weren't quite done. We channeled Sun Tzu further and considered how our enemy might circumvent the hospital's data protection ecosystem. We didn't need to look any further than the **MGM attack** to identify a vector that can't be stopped by any layer of digital security: social engineering.

To protect against this, instead of employing a system, we employed process. Recovery requests submitted to the 24x7x365 P1 Protect service desk would require a quorum. Before any restore overwrites or restores to alternate sources were conducted, support technicians would require sign-off from multiple pre-approved individuals using designated contact methods.

No environment can ever be 100% secure from an attack, but with P1 Protect, the hospital is well-prepared to respond to ransomware threats across its entire infrastructure. Whether protecting workloads in their on-premises data center, M365 tenant, or safeguarding critical assets in the public cloud, P1 Protect ensures that if disaster strikes, and they ever have to recover, they can.

P1 Technologies

P1 Technologies is an innovative consulting team of enterprise architects with deep cloud expertise. We're focused on simplifying and automating workloads, so that our customers can focus on their business goals.

aws partner network

p1technologies.com

310.546.6071
sales@p1technologies.com
3701 Highland Ave, Suite 300
Manhattan Beach, CA 90266