CASE STUDY

Finding the Cure for Swelling Cyber Threats

As the result of embracing more cloud-based platforms and IoT, health care system IT environments have become increasingly complex and susceptible to cyber attacks. Learn how one health care system tapped Trustwave to diagnose its security weaknesses, improve protocols and team up to detect cyber threats before they could cause major damage.

Trustwave®

Client Spotlight

This California-based regional health care system is on the forefront of delivering innovative medical techniques through state-of-the art technology to improve the health and well-being of the community it serves. It needed a modern security strategy to help reduce new cyber risks brought about by increased reliance on cloud platforms and IoT.

The Challenge

After undergoing a third-party risk assessment, this health care system realized it needed to improve its cybersecurity posture to meet stringent compliance demands. Yet with only three dedicated security personnel, they knew they couldn't do it alone.

Experiencing nearly 12 million security events per day, there was simply no way the small IT team could correlate and analyze the sheer volume of event data to effectively triage alerts. With an increasingly complex environment — monitoring IoT devices at patient bedsides, recently adopting cloud platforms such as MyChart and EPIC, and managing the realities of a remote workforce — the team recognized it couldn't execute a robust threat detection and response strategy while also staying focused on operationalizing its evolving system architecture. It needed a true partner — an industry-leading MSSP who embraced both HIPAA and NIST framework requirements — to integrate all of the moving parts. Only then could it make strides toward the cybersecurity program maturity it sought as part of its overall digital transformation efforts.

The Solution

The organization asked Trustwave to test its defenses through threat hunting and phishing exercises. The successful conclusion of these engagements led to a tabletop exercise with company stakeholders to create escalation protocols. By involving decision-makers outside of IT, this crucial planning process increased the company executives' awareness of important security and compliance-related activities and validated the role all parties play in their success.

Meanwhile, Trustwave seamlessly set up the environment to collect data from network devices and servers to be parsed for analysis in the cloud, enabling integration with other cloud-based company data and cloud-based alerts. With access to the cloud-based Trustwave Fusion platform, the client's security team could see all of its alerts triaged by severity, making it easier to zero in on and respond to incidents that could compromise their 500+ servers and network devices and organization data.

Ongoing penetration testing and vulnerability scanning conducted by Trustwave combined with 24x7 monitoring offer the organization peace of mind that their security controls are working and compliant with industry frameworks and standards. Of the partnership, its cybersecurity lead said, "We just finished our year-end compliance audit, finding that all high-priority risks from the year prior had been mitigated. We owe much of this successful transformation to Trustwave."

> “*With 12 million events per day, the fear of being compromised is real. Trustwave helps us funnel those into 12 priority incidents, making our security response stronger and less overwhelming for our team.*”
>
> — Cybersecurity Lead

Trustwave®