OPSUS DEFEND

Security-as-a-Service

– Powered by Fortified Health Security

THE CHALLENGE: MAINTAINING A STRONG SECURITY STANCE AGAINST EVOLVING THREATS

The threats to healthcare IT and patient data are constantly multiplying and evolving. Traditional, one-time "analyze and remediate" services cannot keep pace. By the time the recommendations from a risk analysis have been implemented, they are already out-of-date. Costly "after event" services are useful for containing and eradicating security threats which have already penetrated, but they do not set you up for long-term protection and success.

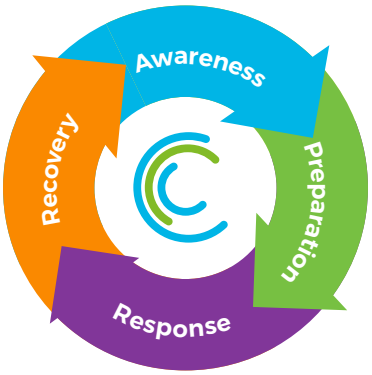
The best protection is to maintain a team of organizationally enabled security experts, but this can be difficult to build and often expensive. Healthcare organizations need a way to meet these ever-evolving security threats to patient data and meet compliance with federal regulations.

THE ANSWER: OPSUS DEFEND

OpSus Defend is a suite of managed security services delivered from the OpSus Healthcare Cloud, and powered by Fortified Health Security. OpSus Defend allows Healthcare IT to add layers of professionally-managed security protection and monitoring to their on-premises or cloud-based systems infrastructure. Available as individual services or bundled into packages, OpSus Defend offers HIPAA Risk Analysis, Security Information and Event Monitoring (SIEM), Penetration Testing, Data Loss Prevention, and Vulnerability Threat Management (VTM).

ADAPT TO THREATS WITH MANAGED SECURITY SERVICES

OpSus Defend transitions one-time services into continuous protection. With monthly technical and non-technical checkpoints, and perpetual threat monitoring, security becomes a robust layer of evolving defense. Our approach to risk mitigation never ends, but rather continues to improve with an awareness, preparation, response, and recovery cycle. We work with you to discover, diagnose, remediate, and understand all the threats and areas of concern in your environment as they arise.



ALL OPSUS DEFEND SERVICES INCLUDE:

- Continuous Monitoring
- Monthly Technical Checkpoints
- Monthly Non-Technical Checkpoints
- Progress and Trending Reports

OpSusDefend
Powered by Fortified Health Security

CloudWave
Healthcare IT Solutions

CLOUDWAVE 100 Crowley Drive, Marlborough, MA 01752 877-991-1991 gocloudwave.com

HIPAA RISK ANALYSIS

HIPAA Risk Analysis is a rigorous and detailed identification and prioritization of key risks currently facing healthcare organizations. Our Risk Analysis explores the likelihood of a breach and the magnitude of its potential impact by assessing the physical, administrative, and technical information security controls and safeguards outlined by the HIPAA Security Rule.

SECURITY INFORMATION EVENT MONITORING

SIEM provides 24/7 compliance monitoring—including relevant security and system audit events. SIEM not only provides compliance monitoring but also monitors all relevant security and system audit events—including those created by IT Staff. This complete separation of duty will aid response to complicated issues that otherwise may have gone unnoticed. HIPAA specifically mentions event logs as an important vehicle to meet compliance and requires covered entities to collect, analyze, preserve, alert, and report on system and application security event logs generated by all relevant systems.

PENETRATION TESTING

Penetration testing is a proven methodology that replicates real-world attack scenarios, testing your IT infrastructure so that you can protect confidential data from today's ever-evolving threats. OpSus Defend's penetration testing is carried out through seven stages, beginning with scope and definition and concluding with project clean-up and report delivery. This staged approached offers a consistent and reliable testing process. OpSus and Fortified test in four different ways: external, internal, wireless, and application.

VULNERABILITY THREAT MANAGEMENT

VTM provides continuous visibility to vulnerabilities through monthly scanning. As opposed to one time scans, continuous VTM eliminates a "snapshot in time" approach. The results of these scans are viewable via our proprietary dashboard.

DATA LOSS PREVENTION

Data Loss Prevention (DLP) gives you ultimate visibility into where and how your sensitive data is traversing your environment. This tool is dynamic in nature, allowing you to proactively manage where sensitive data is sent and how it is received. DLP tools provide a number of mechanisms to analyze risks to ePHI per the HIPAA Security Rule and limit ePHI access to the "Minimum Necessary."

- Discover ePHI stored on laptops, workstations and servers that are encrypted
- Scrub ePHI being emailed out of your organization
- Detect ePHI being transformed out of your organization in unencrypted FTP and similar web-based protocols
- Audit and control ePHI being copied to USB devices or burned to CDs or DVDs

Fortified HEALTH SECURITY

ABOUT FORTIFIED HEALTH SECURITY

Fortified Health Security is a team of security professionals dedicated to healthcare. Their experienced staff monitors, identifies, and manages cybersecurity risks on an ongoing basis, resulting in a stronger security stance.

Fortified's cybersecurity team assesses risks, implements safeguards to protect sensitive patient information, and assists with compliance with state and federal regulations.

CloudWave works with Fortified to match security resources with technical expertise to help customers address their security concerns.

For more information about our services, please contact your CloudWave Sales Team at 877-991-1991, or send an email to customersfirst@gocloudwave.com.

OpSus CloudCare

CloudWave offers a complete suite of services to provide customers with options for end-to-end MEDITECH and enterprise systems support and management.

CloudWave Healthcare IT Solutions