CYBERSECURITY PURPOSE-BUILT FOR MSP CUSTOMERS

Small businesses dealing with PHI often struggle to manage their security compliance requirements. Compliance standards are often complex, dense and require multiple skill sets to understand. The average business owner dealing with PHI doesn't have the time or resources to effectively manage these compliance requirements on top of their other responsibilities. Today, many vendors will deliver "compliance" in a box for small businesses. This ends up being a package of documents (never to be read) and some technology that is slapped into place. This delivers a "magical" state of compliance which, like most magic tricks, ends up as a sleight of hand.

The Network Defender sensor helps small businesses meet the HIPAA and HITECH requirements in a number of ways. Below is a table with the specific requirement and a short description of how Network Defender supports the security objective:

Network Defender® supports HIPAA/ HITECH requirements as follows:

- Continuous risk assessment of your network traffic (both in and out)
- On demand reporting/audit reports
- Automated incident response
- Enforcement of access to Protected Health Information (PHI)
- Alerting on suspicious activity and enabling users to take action on those alerts
- Isolating Health Care Clearinghouse Function
- Continuous monitoring of all network activity

NIST 171 Reference	Family	NIST Requirement/Short Description	Network Defender Feature/Description
Risk Management 163.308(a)(1)(ii)(A)	Risk Analysis	Practices are required to conduct an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. This process is intended to identify current security risks.	The Network Defender sensor monitors every packet of traffic that traverses the firewall and assigns a risk score to the traffic. This allows the customer to clearly demonstrate an ongoing risk assessment of every single bit of network traffic in fully auditable form.
Risk Management 163.308(a)(1)(ii)(B)	Risk Management	Practices are required to implement security measures sufficient to reduce risks and vulnerabilities identified during the risk analysis and to stay compliant with HIPAA security standards. This process is intended to ensure ongoing control of security risks.	Every Network Defender sensor has a number of on demand audit reports that support operations and investigations as required. Additionally, the policy designer allows the customer to adjust the performance of the standard in accordance with the identified risk.
Administrative Safeguards 164.308(a)(1)(ii)(D)	Information System Activity Review	The purpose is to ensure that someone is regularly monitoring the practice's systems for any unauthorized access.	The Network Defender sensor monitors, scores and takes action on all of your network traffic 24/7/365 and provides you the report to prove it.
Information Access Management 164.308(a)(4)	Isolating Health Care Clearinghouse Function	Electronic PHI processed by the clearinghouse is isolated from the other information that the practice processes.	The core of the Network Defender sensor is the use of machine learning to integrate, correlate and report on inappropriate, suspicious or unusual activity directed at the sensitive nodes on your network.

NIST 171 Reference	Family	NIST Requirement/Short Description	Network Defender Feature/Description
Information Access Management 164.308(a)(4)	Audit and Accountability	IT systems are set up to automatically logout a user after a short period of inactivity and requires a password to re-enter the application. IT system is configured to only allow the user access to predetermined sets or areas of information relevant to their job duties.	The Network Defender SAAS environment provides the full audit reduction capabilities and the user interface supports the on-demand analysis and reporting capabilities that allow you to track who from the outside-connected to what data on the inside.
Security Awareness and Training 164.308(a)(5)	Protection from Malicious Software	Computer viruses and attacks pose a significant risk to any business or medical practice. Practices need to be vigilant regarding limiting the use of the internet and downloading software programs by its employees.	The core of the Network Defender sensor is the use of machine learning to integrate, correlate and report on inappropriate, suspicious or unusual activity directed at your network. Our method of action compliments endpoint management and antivirus capabilities to reduce risk to your network.
Administrative Safeguards 164.308(a)(6)	Security Incident Procedures	A security incident is the “attempted or successful unauthorized access, use or disclosure, modification, or destruction of information or IT operating systems. Examples may include stolen passwords, corrupted back-up tapes, virus attacks, accounts being used by another individual, failure to terminate an account of a former employee and unauthorized use of systems.	The Network Defender scoring system allows users to create policies/standards to manage their network communications traffic and take the user directed action (block, notify, permit) on an ongoing basis. The power of the sensor is that it delivers incident response capability 24 hours a day/7 days a week/365 days a year.
Contingency Planning 164.308(a)(8)	Evaluation Policy	Practice must periodically evaluate their security plans and procedures to ensure their continued effectiveness. A technical evaluation should be conducted by IT experts or your vendor due to the complexity of computer systems.	Every Network Defender sensor has a number of on demand reports that support continuous monitoring processes for your existing controls and in most cases obviates the need for 3rd party reviews for many of your technical controls.
Audit Controls 164.312(b)	Audit Controls	Implement hardware, software and procedural mechanisms the record and examine activity in information systems that contain or use ePHI	Every Network Defender sensor has a number of on demand audit reports that support operations and investigations as required. Additionally, the policy designer allows the customer to adjust the performance of the standard in accordance with the identified risk.