CYBERSECURITY PURPOSE-BUILT FOR SMALL & MEDIUM BUSINESSES

Small businesses often struggle to manage the variety of compliance requirements they encounter. Compliance standards are often complex, dense and require multiple skill sets to understand. The average business owner 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.

Network Defender® supports small business compliance with NIST 171 by enabling:

- Monitor and control of network connections
- Audit and reporting of network connections
- Limiting access to sensitive systems
- Protecting communications and systems
- Alerting on suspicious activity and enabling users to take action on those alerts
- Identifying unauthorized use of systems

In order to protect its data, the Department of Defense has placed an enormous focus on ensuring that its vendors are compliant with a set of complex security standards contained within the National Institute of Security and Technology Special Publication 171 (NIST 171). Multiple malicious entities have leveraged the weaker security of DoD's vendors to steal critical information and data. However, small businesses have struggled with developing effective solutions that can meet both the complex requirements as well as their yearly budgets.

The Network Defender sensor helps small businesses meet these requirements in a number of ways. Below is a table with the specific NIST 171 requirement and a short description of how Network Defender supports the security objective:

NIST 171 Reference	Family	NIST Requirement/Short Description	Network Defender Feature/Description
3.1.12	Access Control	Monitor and control remote access sessions.	The Network Defender sensor monitors every packet inbound or outbound through the firewall and can be used to block inappropriate traffic.
3.3.1	Audit and Accoountability	Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	Every Network Defender sensor has a number of on demand audit reports that support operations and investigations as required.
3.3.3	Audit and Accountability	Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	The core of the Network Defender sensor is the use of machine learning to integrate, correlate and report on inappropriate, suspicious or unusual activity AND take the necessary actions to prevent that traffic from harming your network.

NIST 171 Reference	Family	NIST Requirement/Short Description	Network Defender Feature/Description
3.3.5	Audit and Accountability	Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	The core of the Network Defender sensor is the use of machine learning to integrate, correlate and report on inappropriate, suspicious or unusual activity AND take the necessary actions to prevent that traffic from harming your network.
3.3.6	Audit and Accountability	Provide audit reduction and report generation to support on-demand analysis and reporting.	The Network Defender SAAS environment provides the full audit reduction capabilities and the user interface supports the on-demand analysis and reporting capabilities.
3.3.8	Audit and Accountability	Protect audit information and audit tools from unauthorized access, modification, and deletion.	Access to the user environment is restricted to only those users with explicit permission to monitor the audit reports. All user activities are tracked. Additionally, users do not have the ability to access, modify or delete the data or reports.
3.3.9	Audit and Accountability	Limit management of audit functionality to a subset of privileged users.	All audit reports are limited to a subset of identified privileged users.
3.13.1	Systems and Communication Protection	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	The Network Defender sensor monitors every packet that transits the device it is attached to 24 hours a day, 7 days a week, 365 days per year.
3.13.6	Systems and Communication Protection	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	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.
3.14.3	Systems and Information Integrity	Monitor information system security alerts and advisories and take appropriate actions in response.	The Network Defender sensor automates this process for you continuously. All traffic is scored on a scale that is 0-9 and the appropriate actions are driven by the score. So, customers don't have to be a security analyst in order to make effective use of the tool.
3.14.6	Systems and Information Integrity	Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	All traffic transiting the firewall is monitored and scored. The score is derived from the monitoring of XX number of sources and behaviors and has proven to be very effective at picking up "bad" behaviors BEFORE signatures and alerts are sent to customers.
3.14.7	Systems and Information Integrity	Identify unauthorized use of the information system.	The Network Defender sensor doesn't just identify unauthorized use of the information system it can stop and security incident from turning into a security breach. All traffic is scored and when unauthorized traffic is identified it can be stopped automatically without user intervention.