Business Benefits

- Align medical device procurement strategy to network security so that gaps are identified and mitigated before the device is authorized to operate.
- Detect threats faster using an integrated security solution with curated automation
- Increase visibility into medical device activity by monitoring their communications and behaviors
- Improve identification of medical devices by profiling function, criticality, state and location
- Improve the ability to mitigate varying levels of medical device risk through network policy, automated response and classification of risk to mission
- Improve risk management focused on patient care by analyzing and correlating IoT security data to inform stakeholders of risks to patient care

For more information about the Red River Medical Device Isolation Architecture solution contact your Red River account team by phone 800.769.3060 or email mdia@redriver.com.

Red River

Medical Device Isolation Architecture

Healthcare organizations are rapidly adopting networked medical devices to provide innovative approaches to patient care. These devices provide direct treatment, diagnostics, patient care monitoring and control of vital infrastructure and utility systems.

Without clear Food and Drug Administration (FDA) regulation and industry manufacturing standards, these devices often contain vulnerable hardware and software, which attackers can exploit. The combination of vulnerable medical devices and proximity to patients poses a significant risk to patient care and the healthcare mission. A new network based approach is needed to establish trust and securely integrate medical devices into healthcare networks.

Vulnerable Medical Devices Are Being Targeted

Medical devices are often deployed in an unprotected state, and manufacturers have little incentive to provide security updates despite the discovery of new vulnerabilities. Once these devices are deployed, biomed administrators are typically unable or afraid to make modifications that could compromise the intended functionality or increase the risk of liability due to a malfunction. These are the same devices responsible for the safety and health of the patients they serve. A compromised device can result in a failure of the treatment or even death. The inability to secure vulnerable medical devices has allowed cyber criminals to use them to their advantage in attack campaigns.

With the stakes so high, healthcare delivery organizations are left with an enormous problem: how to ensure the safety of their patients—protecting both life and privacy—while having little control over the security of the devices used to treat and care for them.

A comprehensive network access and policy control solution can solve these challenges by addressing the following key requirements:

- Alignment of medical device risk to mission risk
- Identification, classification and registration of all devices that connect to the network
- Strong authentication and authorization for all medical and supporting staff
- Effective segmentation and enforcement controls at the point of access and throughout the network
- Continuous monitoring and visibility for all network access, network behavior and vulnerabilities
- Ability to detect threats and provide automated alerts and responses

A DIRECT APPROACH TO SECURING MEDICAL DEVICES

Red River developed a Medical Device Isolation Architecture (MDIA) to address the unique challenge of securing medical devices with minimal impact to the delivery of patient care. The Red River MDIA is an agentless solution that leverages existing network infrastructure investments to continuously identify, classify, segment, monitor and adaptively secure medical devices with minimal impact at scale. MDIA is built upon key technology partnerships from Red River, Cisco, Tenable and Splunk.

Gain Visibility

We start by identifying and classifying all devices connected to the network in order to understand what devices and associated vulnerabilities are present. Using existing wired, and wireless network access devices, our solution continuously performs passive device profiling, vulnerability detection and machine learning of network behavior to develop a medical device security profile for each device.

Red River at a Glance

- Founded in 1995
- Privately-Held
- ISO 9001:2015 Certified
- SOC 2 Type 1 certified
- Corporate Headquarters in Claremont, NH
- Federal Office in Reston, VA
- Innovation Center in Austin, TX
- Development Office in Sacramento, CA

About Red River

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing more than 20 years of experience and mission critical expertise in security, networking, analytics, collaboration, mobility and cloud solutions.

LEARN MORE

For more information please call 800.769.3060 or visit redriver.com

Follow us on Twitter: @ThinkRed

The medical device security profile aids network, security and biomed administrators in onboarding medical devices and classifying their risk to the healthcare mission. The security profile collects and correlates device type, 360-degree communication behavior, security posture, location, procurement status and hardware lifecycle in a single near real-time view for better decision-making. The Red River MDIA solution uses the security profile to evaluate and assign an initial mission risk classification, network authentication policy and network authorization policy to the device.

Protection through Segmentation

Once the authentication and authorization policy for a medical device is defined, the Red River MDIA solution applies adaptive, scalable segmentation policies at the network access, datacenter and campus edge using multiple controls (Downloadable ACL, VLAN, Named ACL and Software Defined Access). When a device moves to a different location, the segmentation policy follows, allowing for consistent application of security policy regardless of access method (wired, wireless).

Identify and Contain Threats

To protect the medical devices and the healthcare network from attack, the Red River MDIA solution continuously analyzes device security posture using network behavioral analysis, Next Generation Intrusion Prevention and passive vulnerability detection. If the security posture of a device changes due to attack or newly discovered vulnerabilities, the solution can automatically adjust the devices mission risk classification, add security controls, alert administrators and automate a containment or restriction response.

MEDICAL ISOLATION ARCHITECTURE TECHNOLOGIES

Cisco Identity Services Engine (ISE): Centralized Network Access Control and policy management software

Cisco Stealthwatch: Behavioral analysis technology

Cisco Firepower: Next generation firewall, intrusion prevention and anti-malware defense

Tenable Security Center CV: Passive identification and reporting of medical device vulnerabilities

Splunk Enterprise: Customizable and scalable monitoring and reporting

RED RIVER
Corporate Headquarters
21 Water St., Suite 500
Claremont, NH 03743
800.769.3060 toll free
603.448.8880 phone
603.448.8844 fax

www.redriver.com

Red River