IoT - Device Isolation Architecture

Modern organizations are transforming their business strategies through rapid adoption of new network connected devices and technologies known as the Internet of Things (IoT). These devices add capabilities and provide control of critical systems in manufacturing, energy, transportation, retail, healthcare, communications, government and education networks.

Business Benefits

- Understand how IoT device risk impacts mission risk and compliance
- Automatically identify, classify and secure IoT assets connected to the network.
- Gain visibility into IoT device risk through continuous vulnerability detection behavioral analysis
- Secure vulnerable IoT devices with automated adaptive security controls
- Detect and contain threats faster using an integrated solution

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

Red River

Without clear regulation and industry manufacturing standards, networked IoT devices often contain vulnerable hardware, software and configurations, which cyber attackers can exploit. The combination of vulnerable devices and proximity to users and critical business processes poses a significant risk to an organization's mission. A new network-based approach is needed to establish trust and securely integrate IoT devices into modern networks.

Vulnerable IoT Devices Are Being Targeted

IoT 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, 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. The inability to secure vulnerable devices has allowed cyber criminals to use them to their advantage in attack campaigns.

With the stakes so high, organizations are left with an enormous problem:

How do we ensure the safety of our data and systems, while having little control over the security of the devices used to streamline business processes?

Red River has determined that the answer to this enigma is a comprehensive network access and policy control solution can solve these challenges by addressing the following key requirements:

- Alignment of device risk to mission risk
- Identification, classification and registration of all devices that connect to the network
- Strong authentication and authorization for all supporting staff, contractors and guests
- 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 curated responses

A DIRECT APPROACH TO SECURING DEVICES

Red River developed a Device Isolation Architecture (DIA) to address the unique challenge of securing devices with minimal impact to the organization implementing this robust security solution. The Red River DIA is an **agentless solution** that leverages existing network infrastructure investments to continuously **identify**, **classify**, **segment**, **monitor** and **adaptively secure** devices with minimal impact at scale. DIA is built upon key technology partnerships from the industry's leading OEM providers.

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**,

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

our solution continuously performs passive device profiling, vulnerability detection and machine learning of network behavior to develop a device security profile for each device.

The device security profile aids network, security and network administrators in onboarding devices and classifying their risk to the organization's mission. The security profile collects and correlates device type, 360-degree communication behavior, security posture, location, and procurement status as well as hardware lifecycle in a single near real-time view for better decision-making.

The Red River DIA 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

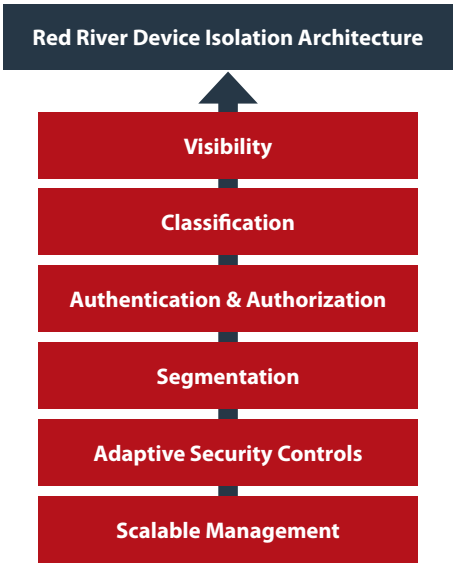
Once the authentication and authorization policy for a device is defined, the Red River DIA solution applies adaptive, scalable segmentation policies at the network access, datacenter and campus edge using multiple controls (Downloadable ACL, VLAN, Named ACL and Software Defined Access). When a device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

Identify and Contain Threats

To protect the devices and the network from attack, the Red River DIA solution continuously analyzes device security posture using network behavioral analysis, next generation threat 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.

ISOLATION ARCHITECTURE TECHNOLOGIES

- Centralized Network Access Control and policy management software
- Behavioral analysis technology
- Next generation firewall, intrusion prevention and anti-malware defense
- Passive identification and reporting of medical device vulnerabilities
- Advanced data and security analytics
- Next generation compliance monitoring and assessment suite



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