SPECIAL NEWS

Gartner Lists Blue Ridge Networks, Inc. as Sample Vendor in their Hype Cycle for Cyber-Physical Systems Security, 2024

Overview

Cyber-Physical Systems (CPS) represent the convergence of computation, networking, and physical processes. These systems utilize embedded computers and networks to monitor and control physical operations, often employing feedback loops that allow physical events to influence computations and vice versa.

According to Gartner's Hype Cycle for Cyber-Physical Systems Security, 2024, "The impacts of the globally evolving regulatory environments, ransomware, cyberattacks and deployment of CPS in critical infrastructure have changed how CPS-related risk manifests in organizations." This highlights a more keen focus on CPS and the vital importance of alignment and harmonization between Information Technology (IT) and Operational Technology (OT) cybersecurity solutions.

The Gartner Hype Cycle for CPS Security, 2024 shares a comprehensive priority matrix for CPS, in which zoning and segmentation play a vital role.

Why are Zoning and Segmentation Important?

CPS zoning and segmentation solutions assist in outlining current network configurations. They help with clarifying firewall settings, concealing CPS networks from public discovery, and ensuring that CPS components communicate solely when essential. This approach mitigates the risk of intellectual property theft and prevents the loss of oversight or control over physical operations due to malware attacks that:

- Travel North-South = Navigating from IT systems to production or mission-critical environments.
- Travel East-West = Navigating laterally
- Can be exploited by insider threat actors with physical access to CPS (South-North)

What's Creating the Need for Zoning & Segmentation?

The evolving threat landscape's main considerations include:

- Increased ransomware attacks that prompt entities shut down operations.
- Concerns about the potential spread of malware to cyber-physical systems (CPS) environments.
- Growing awareness about maintaining large trust zones within facilities is an ineffective strategy for managing risks. This creates a more accessible battle space.
- The need for more effective methods to thwart a cyber attacker's ability to move laterally within a system. Dividing networks into smaller segments or zones reduces the battle space for improved management and access control.

Zoning and segmentation are not just practical responses but are also foundational recommendations outlined in industry-recognized security frameworks, including NIST SP 800-82 rev3 and IEC 62443. Adherence to various industry regulations and standards, such as NERC-CIP, mandates that organizations implement network segmentation as part of their security protocols. Compliance is crucial, as it helps avoid penalties, fosters customer trust, and protects sensitive information.

What Are the Barriers to Achieving Effective Zoning & Segmentation

- **Legacy Systems/Security Gaps:** Today's security considerations were not factors for numerous legacy systems when they were originally designed. These systems lack essential features to support effective zoning and segmentation without disrupting vital operations.
- **Visibility Issues and Complexity:** Insufficient visibility into network components and unknown interdependencies can create obstacles, as various components may rely on one another to function properly.
- **Operational Complexity:** Implementing zoning and segmentation can add layers of complexity to existing network operations.
- **Resource and Expertise Limitations:** Many organizations within critical process sectors struggle with constrained budgets and may lack personnel who possess the necessary security and engineering expertise.
- **Operational Constraints:** In sectors like energy and manufacturing, any downtime or disruptions can lead to significant financial losses and pose serious safety risks.

How to Overcome These Barriers

- **Asset Identification:** To effectively enhance network security and visibility, organizations should deploy CPS Protection Platforms to discover all CPS assets within their environments. This initial step provides critical insights into existing network topologies, allowing for better management.
- **Zone Collaboration - IT/OT Harmonization:** Solutions architects should collaborate with engineering teams to create security zones. Together, they must consider elements such as physical process loops, the criticality of operations, safety, risk profiles, and operational constraints. Each security zone must serve a specific purpose and be fortified with appropriate levels of security controls.
- **Zoning Technologies:** To enforce strict segmentation between these zones, organizations can utilize firewalls, routers, and switches. Additionally, adopting network segmentation technologies like virtual LANs will help create isolated network segments, effectively controlling traffic flow between different zones.
- **Secure Access:** Implementing the principle of least privilege is also crucial. Remember to limit user access rights and privileges to only those that are necessary for their roles to minimize potential security risks. Lastly, vigilant monitoring and logging of network traffic within each security zone facilitates the detection of suspicious activities, aiding in timely incident response efforts.

Conclusion

The deployment of Cyber-Physical System (CPS) Protection Platforms serves as the cornerstone for discovering CPS assets and understanding network topologies, which is essential for effective management. Robust CPS security must include zoning and segmentation to enhance network security and to limit access. This will help to minimize operational downtimes and/or financial losses for industries such as manufacturing and energy.

The establishment of security zones, guided by network segmentation collaboration between solutions architects and engineering teams, allows organizations to address operational constraints and safety measures strategically and to enforce strict traffic control, thereby bolstering their overall security posture.

Implementing the principle of least privilege and maintaining vigilant monitoring and logging practices further contribute to a strong defense mechanism. These strategies collectively empower organizations to proactively identify and respond to potential threats, resulting in a more secure and resilient operational environment, thus protecting critical assets and ensuring safe continuous operations.

> Blue Ridge Networks' LinkGuard solution is emphasized as a key player for CPS security, effectively reducing attack surfaces while ensuring secure data transit across user devices. Recognized by Gartner as "Early Mainstream," LinkGuard demonstrates scalability and immediate applicability, making it a viable option for both private and public sector entities facing challenges with legacy systems and budget constraints.

Learn More About LinkGuard™

About Us

Blue Ridge Networks, Inc., is a proven and trusted provider of effective CPS/OT/IT cybersecurity solutions. Our zero-trust quantum resistant "CyberCloak™" capabilities are protocol agnostic, compatible with legacy systems, and deploy quickly with minimal overhead. We protect continuous operations by enabling secure remote access while preventing external network infiltration and mission-critical data exfiltration.

Regulated, Commercial, and Industrial organizations have trusted Blue Ridge Networks for over 20 years to prevent exploits and receive continuous returns on their investments while achieving uninterrupted operational efficiency.

BLUERIDGE® NETWORKS

1-800-704-5234
sales@blueridgenetworks.com
BlueRidgeNetworks.com