RHEL 7 Warehouse Management System: Cybersecurity Monitoring Deployment

Project Author

Charlie Hofner
LinkedIn
IT Professional specializing in cybersecurity and infrastructure deployments.

Overview

This project documents the deployment of cybersecurity monitoring tools on Red Hat Enterprise Linux (RHEL) 7.0 servers hosting a Warehouse Management System (WMS). A total of 12 servers were involved: 6 development (dev) servers and 6 production (prod) servers. The servers were approaching End-of-Life (EOL) status, prompting a proactive security hardening effort ahead of potential cloud migration mandates. Key focus: Installing Arctic Wolf Networks Linux agents for managed detection and response (MDR), alongside ConnectSecure for automated vulnerability management and compliance monitoring.

Goals: - Enhance threat detection on legacy infrastructure. - Identify and mitigate vulnerabilities before EOL enforcement. - Ensure minimal downtime for critical WMS operations.

Tech Stack: - OS: RHEL 7.0 - Monitoring: Arctic Wolf Linux Agent, ConnectSecure - Environment: On-premises servers (warehouse ops)

Background

Our WMS ran on RHEL 7 servers, which reached end of maintenance support in June 2024 (with optional Extended Life Cycle Support available until 2028/2029 depending on add-ons). An upgrade to RHEL 8 would have provided full maintenance support until May 2029, offering a more secure on-premises path. However, the software vendor showed limited interest in supporting an OS uplift and appeared focused on migrating customers to their cloud-hosted product—likely at a higher long-term cost. Vendor support for the on-premises version was inconsistent, leaving security gaps in an unmonitored legacy setup. This deployment added layered monitoring without disrupting 24/7 warehouse workflows, buying time while bridging the EOL risks.

Project Timeline

- **Start Date:** Second week of January 2025
- **Completion Date:** End of January 2025
- **Scope:** 6 dev servers + 6 prod servers (12 total)
- **Approach:**
    - Initial deployment and testing on the 6 dev servers.
    - Monitoring period of one week to observe stability, performance impact, and alert accuracy.
    - Final rollout to the 6 prod servers after successful validation on dev.

Prerequisites

- Root access to RHEL 7.0 servers.
- Arctic Wolf Networks account/subscription for agent licensing.
- ConnectSecure account (MSP-focused platform; agent deploy via portal-generated scripts).
- Basic package management (yum for RHEL 7).
- Firewall rules allowing outbound traffic for agent telemetry (e.g., ports 443/TCP for Arctic Wolf and ConnectSecure).

Note: All steps were first tested in the dev environment before production rollout.

Deployment Steps

1. Arctic Wolf Linux Agent Installation

Arctic Wolf's agent provides endpoint detection, log collection, and MDR services tailored for Linux.

1. **Download the Agent Package:**

    - Log in to your Arctic Wolf Console (console.arcticwolf.com).
    - Navigate to **Sensors > Linux** and generate a deployment token.
    - Download the RPM: `aw-sensor-linux-<version>.rpm` (e.g., via wget: `wget https://your-org-sensor-url/aw-sensor-linux-x.x.x.rpm`).

2. **Install the Agent:** ```bash # Verify integrity (optional SHA checksum from Arctic Wolf) sha256sum aw-sensor-linux-x.x.x.rpm

    # Install via yum

    sudo yum localinstall aw-sensor-linux-x.x.x.rpm -y

Configure with your token (replace)

```
sudo /opt/arcticwolf/awagent/bin/awagentctl set-token
```

Start and enable the service

```
sudo systemctl start awagent sudo systemctl enable awagent
```