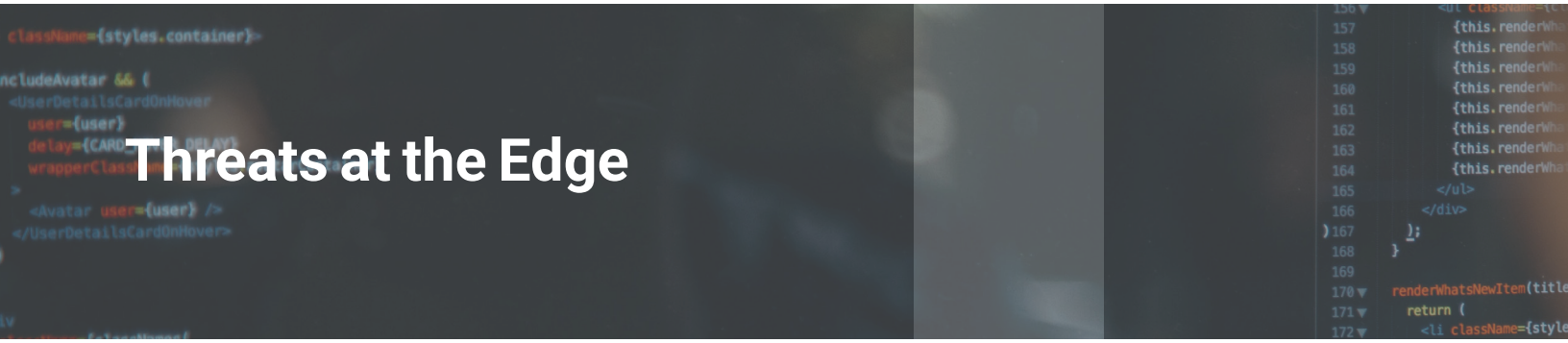
Securing Linux Devices at the Edge

5 Best Practices to Mitigate Risk

WNDRVR



Threats at the Edge

As the world of intelligent systems expands, so does the threat landscape for enterprises, particularly at the network edge where most embedded devices are deployed. The numbers behind digitization and its potential security risks are a cause for concern among even the most seasoned CISOs. IoT Analytics estimates that there are more than 14 billion IoT devices currently deployed.[1] By 2025, IDC expects that number to exceed 55 billion.[2]

The expanding connected universe offers endless opportunities for cybercriminals and hacktivists to exploit. Security company Kaspersky measured 1.51 billion IoT breaches in the first half of 2021 alone.[3] Securing IoT and edge devices requires a unique approach that differs from traditional network and endpoint security. Additionally, there are special security considerations around IoT and edge devices that run on an embedded Linux platform.

In this white paper, we'll take a closer look at security best practices for protecting Linux-based devices at the edge, distilled from the decades of Wind River® experience in building, supporting, and securing embedded Linux devices. Specifically, we'll examine the five best practices for securing Linux devices at the edge: understanding the threat landscape, securing the data, staying current with security updates, automating the security process, and managing the security lifecycle.

> Security company Kaspersky measured 1.51 billion IoT breaches in the first half of 2021 alone.
>
> —Callum Cyrus, *IoT World Today*

1 Hasan, Mohammad, "State of IoT 2022: Number of Connected IoT Devices Growing 18% to 14.4 Billion Globally," IoT Analytics, May 18, 2022
2 Hojlo, Jeffrey, "Future of Industry Ecosystems: Shared Data and Insights," IDC, January 6, 2021
3 Cyrus, Callum, "IoT Cyberattacks Escalate in 2021, According to Kaspersky," IoT World Today, September 17, 2021

1 Understanding Your Threat Landscape

A threat landscape is defined by the total number of cyberthreats that can potentially impact your business, whether the goal of those attacks is data exfiltration, business disruption, extortion, or something else. The first best practice for securing edge devices is to understand which threats can affect those devices. This can be accomplished by focusing on six key questions:

1. What are you protecting?

The most common answer here is data, but you need to dig a level deeper and ask yourself what kinds of data need protection. It could be personally identifiable information (PII), passwords, security data (e.g., encryption keys), device configuration data, and even device-specific data such as the calibration settings on an X-ray machine. Beyond that, you may also be protecting people, your business, or the devices themselves.

2. Which specific threats do you face?

Cyberattacks can take many forms, including unauthorized access, data theft, loss of reputation, and financial theft. Threat identification means not only answering the question of what cybercriminals are after but also determining the type of threat they pose and which common vulnerabilities and exploits (CVEs) they are likely to target.

3. How much risk can you tolerate?

Weighing risk helps you prioritize security efforts. How would data theft affect your business reputation? What happens if an edge device stops working? Could modifying calibration data on an X-ray machine cause harm to a patient? These are the kinds of worst-case scenarios that businesses need to think about when planning a security strategy.

4. Are you bound to regulations or compliance?

Many industries are regulated by federal agencies, industry watchdogs, or simply their own standards for security. It's important to understand what the consequences are — financially and operationally — if your security efforts fall out of compliance.

5. How will you respond to a cyberattack?

Do you have a security playbook that is frequently updated to guide your actions in the event of a cyberattack? Without one, your response may be reactive and chaotic.

6. Who will respond to a cyberattack?

In addition to identifying your actions in the event of a cyberattack, you'll also want to identify your actors. In the case of Linux-based platforms, open source solutions are common, so you may want to include third-party suppliers, community members, and government agencies such as the Cybersecurity Infrastructure & Security Agency (CISA) in addition to your own internal response team.

2 Securing Your Data

The discipline of data security has been around for decades. Most organizations will already have a robust and, in many cases, mature data security strategy in place, one that features a wide variety of security tools structured around the principles of confidentiality, integrity, and availability, known as the CIA Triad.

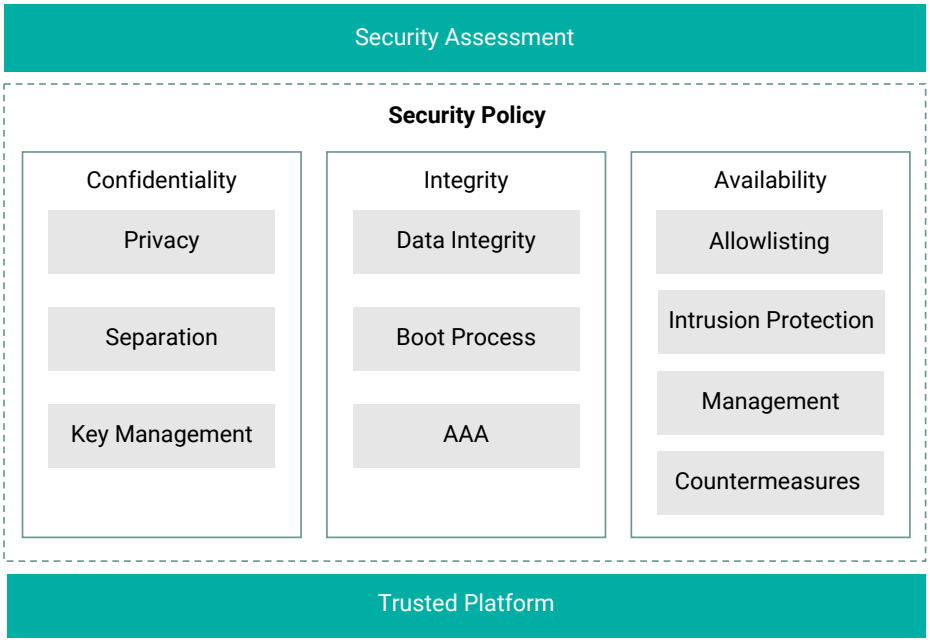
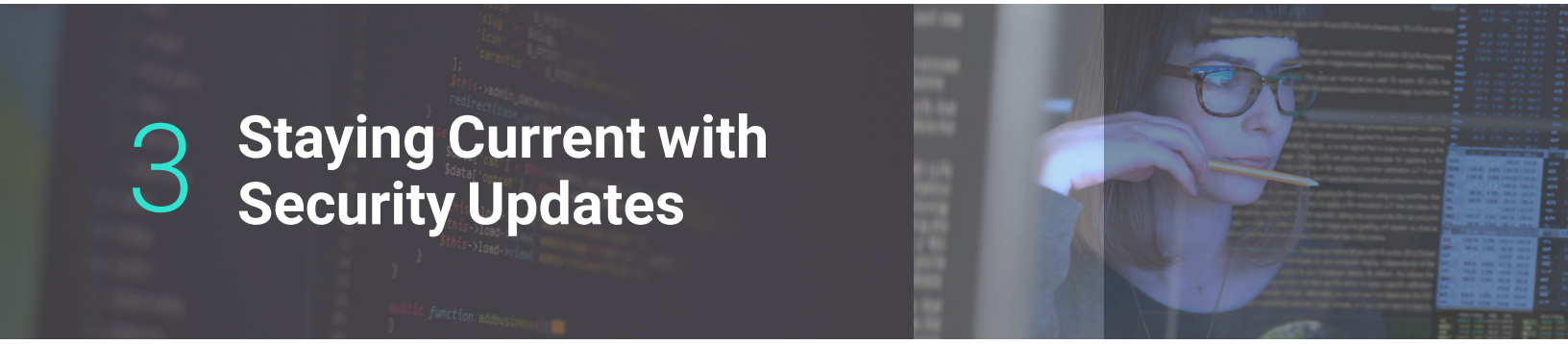


Figure 1. The CIA triad

Putting the Triad to Use

Admittedly, the CIA Triad covers a lot of ground, but it's worthwhile to focus on two specific areas for the purpose of protecting data on Linux-based edge devices:

1. **Patch management:** Organizations must be able to easily update their devices, ideally through some type of over-the-air (OTA), automated process.
2. **Cryptographic sanitization:** Whether they're dealing with a medical device with patient data on it or a manufacturing device holding confidential business data, organizations must have assurance that all data is wiped clean from the device before it is retired.



3 Staying Current with Security Updates

Our third security best practice involves keeping up with changes in the security landscape. In a DevOps-driven world, it's common for businesses to focus on speed-to-market at the expense of security. Over time, this creates a natural security deficit, which is a form of technical debt. Businesses must be careful not to let this (or any) type of technical debt accumulate, as it places them at increased risk of attack.

Particularly for edge-based devices, it's critical that businesses keep current with new updates, new vulnerabilities, and known fixes. Depending on the number of devices and the amount of technical debt accumulated, however, it can be a daunting task to know where to start. The best way to attack the problem is to begin with the CVE prioritization "building blocks" illustrated at right.

Impact

The first step in prioritizing which CVEs to address is to identify their impact. Does the CVE affect a critical component? Can it be launched and controlled remotely or does it require physical access to the device?

Exploitability

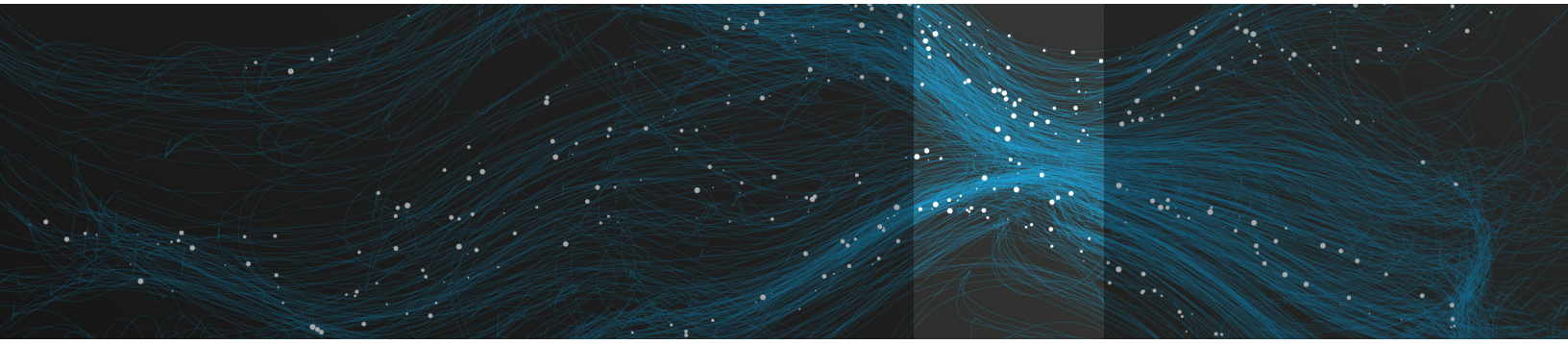
Once you've weighed potential impact, you need to consider how likely it is for the CVE to be exploited. For example, some CVEs are publicly available, while others are more difficult to obtain. For reference, CISA posts a list of known CVEs. The Exploit Prediction Scoring System (EPSS) is another good resource.

Criticality of the System

Security teams should focus on protecting against those vulnerabilities that have the greatest downside or risk for the business. If the CVE can expose critical information (e.g., PII data) or result in a heavy financial loss, it takes on added urgency.

The Building Blocks of CVE Prioritization Decisions

- Impact
- Exploitability
- Criticality of the System
- Ease of Remediation
- Compliance Regulation
- Vulnerability Age
- Vulnerability Score



Ease of Remediation

Similar to the idea of picking the low-hanging fruit first, businesses may want to start addressing their technical debt by starting with time-sensitive vulnerabilities that can be easily fixed.

Compliance Regulation

CVEs that impact your state of regulatory compliance should also be given priority, as these often carry a heavy financial penalty and place future revenue at risk.

Age of the Vulnerability

Unpatched vulnerabilities that have been identified for a long time and that meet your criteria should get significant attention. This is one way of attacking your security-related technical debt, and it should be a priority.

Vulnerability Score

Within the security industry, there is a Common Vulnerability Scoring System (CVSS) assigned to CVEs, presenting a range from 0 (least severe) to 10 (most severe). While businesses should be careful not to make the CVSS score the sole criteria in prioritizing security efforts, it is an important consideration, as the score factors in key issues such as severity of the vulnerability and its potential impact.

> Our third security best practice involves keeping up with changes in the security landscape. In a DevOps-driven world, it's common for businesses to focus on speed-to-market at the expense of security.

4 Automating the Security Process

There were 25,000 unique CVEs identified in 2022,[4] and even a critical CVE can take months for the typical organization to fix.[5] An automated vulnerability scanner can save thousands of hours and secure more of your threat landscape, faster.

That's why our fourth best security practice is having an automated vulnerability scanner. We consider it so important that Wind River® offers an automated vulnerability scanner for free.

While free is a compelling concept all by itself, here are 10 more reasons why the Wind River Studio Linux Services automated vulnerability scanner can help protect your Linux devices at the edge:

1. **CVE lifecycle management:** Our tool integrates seamlessly into your development lifecycle so you can easily identify, assess, prioritize, and remediate (or mitigate) vulnerabilities and reassess/rescan for vulnerabilities later.
2. **Accuracy:** Automatically tap into upstream CVE resources and curate data to your specific market or source so you can be sure of using the latest, most accurate information.
3. **Community updates:** Leverage the latest security information from upstream sources and community members, including updates about the most recent CVEs and known fixes.
4. **Automated scans:** Set scanning automatically (hourly, daily, weekly) and alert security actors with real-time and on-demand notifications.
5. **Efficient triage:** The Wind River vulnerability scanner tool displays CVE data in an easy-to-understand format, including package name/group, license information, color-coded severity, and more so you can more efficiently triage CVEs.
6. **License identification:** Because open source components are common in edge-based Linux devices, you'll instantly see which licenses are being used in your platform.
7. **DevOps integration:** The Wind River security scanning tool is designed to easily integrate into most CI/CD pipelines.
8. **Dashboards:** The dashboard clearly displays data on environmental health, CVEs, and more so that decision makers can quickly find the answers they need.
9. **Reporting:** The artifacts generated by our vulnerability scanner tool can be quickly exported into several formats (e.g., CycloneDX, Microsoft Excel) for convenient reporting.
10. **Secure software bill of materials:** The scanner tool generates a secure SBOM that is protected against unauthorized access.

>> Learn More

4 CVE Details
5 Marshall, David, "Latest AppSec Stats Flash Report from NTT Application Security Finds 50% of Sites Vulnerable in 2021," VMblog.com, February 18, 2022

5 Managing the Security Lifecycle

By now, it should be clear that securing edge devices isn't a one-and-done activity. It's a continuous process that requires planning and action across the life of the device — and this is even more important for Linux-based devices that are exposed to a wide variety of open source licenses and programs. Managing the security lifecycle for edge-based Linux devices can be expressed in five steps: planning, development, deployment, operation, and decommissioning.

1. **Planning:** In this stage, businesses should establish their security policies, identify their security requirements, and populate the skills needed to secure their threat landscape, which may include third-party providers, community members, and partners.
2. **Development:** Businesses in this stage should focus on assembling the right mix of tools to secure and protect their devices. This means choosing the best security hardware and the right security configurations, implementing OS hardening, and integrating additional security solutions.
3. **Deployment:** Once planning and development activities are completed, edge devices are ready for deployment. From this point forward, businesses need to actively monitor for new CVEs, both from their own internal data and from community boards.
4. **Operation:** In this stage of edge device management, businesses need to have mechanisms in place to update devices with new security patches and upgrades, continuously and consistently. Where possible and practical, pushing these updates over the air is ideal.
5. **Decomissioning:** Finally, when devices reach end of life and are retired, businesses need to make sure that they are wiped clean of any proprietary or confidential data.

About Wind River

Wind River is a global leader in embedded Linux systems. For decades, we've helped enterprises from all industries build, deploy, and protect Linux-based systems. We support solutions developed on our own Wind River Linux platform as well as those developed via the open source Yocto Project. For more information on Wind River security scanning services, visit us at www.windriver.com/services/linux/security-scanning.