TuxCare
We Take Care of Linux

WHITEPAPER

Live Patching IoT Devices for Security Protection

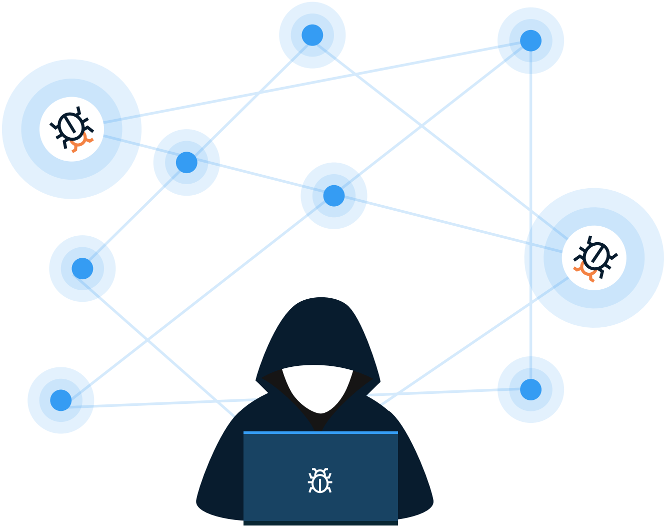
Live Patching IoT Devices for Security Protection

Internet of Everything (IoE) represents connected objects, services, systems, and people across the continuum of everyday life. IoE connects billions of entities embedded with technology that collect and exchange data. These entities may include physical objects, such as cars, refrigerators, thermostats, air traffic control centers, industrial robots, utility meters, transportation hubs, bridges, dams, pipelines, financial institutions, medical equipment, and more. IoE and the internet of things (IoT) also include virtualized network connections between your personal computer, tablet, smartphone, refrigerator, car, thermostat, and millions of other "smart" objects.

When these intelligent objects become hacked, they provide cybercriminals an easy entry into enterprise IT environments. Ransomware attacks increase when these intelligent machines connect to cloud-based analytics platforms. Many of these machines communicate with cloud-based data centers.

According to a report by the Ponemon Institute, unsecured and unprotected IoT devices account for nearly one-quarter of cybersecurity attacks. As of January 1st, 2020, Verizon has analyzed over 160,000 cyberattacks, 72 percent of which were against prominent companies. Being a part of this statistic is a grim outlook for organizations that don't follow the best IoT device compliance frameworks.

Security implications for IoT Devices



Understanding IoT Vulnerabilities

IoT devices and infrastructure can be vulnerable because they reside outside the internal network. They're easy targets for cybercriminals. Many IoT devices run gateway and node software based on Linux, an operating system favored by attackers.

In this environment, the following IoT vulnerabilities result in risk exposure:

- **Operating Systems**

  Each OS open port and available protocol comprise an attack surface area. The code within IoT microcontroller units (MCUs) runs on a “bare metal” basis, with no supporting operating system. Often updating these MCUs continue to be a challenge for organizations.

- **Applications**

  An IoT System on a Chip (SOC) may run multiple app programs, each with potentially exploitable vulnerabilities.

- **Dependencies**

  Apps and OS in IoT devices may have external dependencies and libraries.

- **Communication**

  The IoT is vulnerable to communications-based attacks such as the “man-in-the-middle” and “replay attacks.”

- **Cloud hosting**

  The IoT's supporting cloud infrastructure, connected servers, is also an attack surface.

- **User access**

  Access to devices is a significant vulnerability, especially if attackers can impersonate users without going through the corporate network.

- **Management**

  IoT devices are often not included adequately in inventory and management tools in traditional IT systems. Thus, issues arising in IoT devices can go undetected for long periods.

- **Update process**

  Earlier IoT devices, and to a lesser extent, modern IoT devices, have convoluted update processes that require specialized software, physical access, or a combination of both. Availability of updates is another weak aspect, as some devices will go for prolonged periods without receiving any vendor-supplied updates and can be completely abandoned by the vendor after a short period, *even when vulnerabilities are known to exist for these devices*.

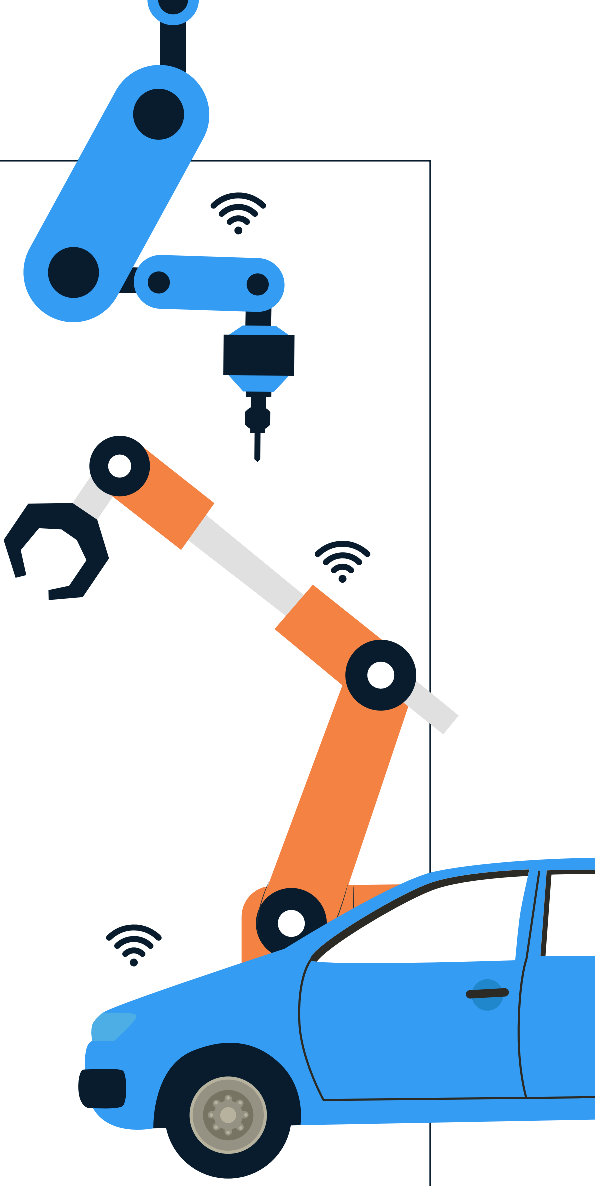
Growth of autonomous cars, robotics, and factory automation

Will autonomous cars and similar vehicles work without an IoT strategy?

The challenge is certainly not the absence of a vision for IoT; instead, it is the absence of centralized engineering standards and protocol. For an autonomous vehicle to communicate with remote IoT devices such as traffic signals, each device within the car must constantly operate and use the most current software application to ensure reliable operation. With the increasing number of connected devices within cars, how can the vehicles themselves stay updated with the latest software and security fixes?

Having real-world information about your customers' needs and preferences fed directly into AI algorithms is the future of customer service. Autonomous vehicles monitoring the welfare of the passengers also has become a critical use case. Specific to diabetic or cancer patients suffering from a medical emergency, the car will have the ability to take them to the closest hospital automatically.

These are all great examples of how IoT technology is being used today to enhance our lives.



Retail

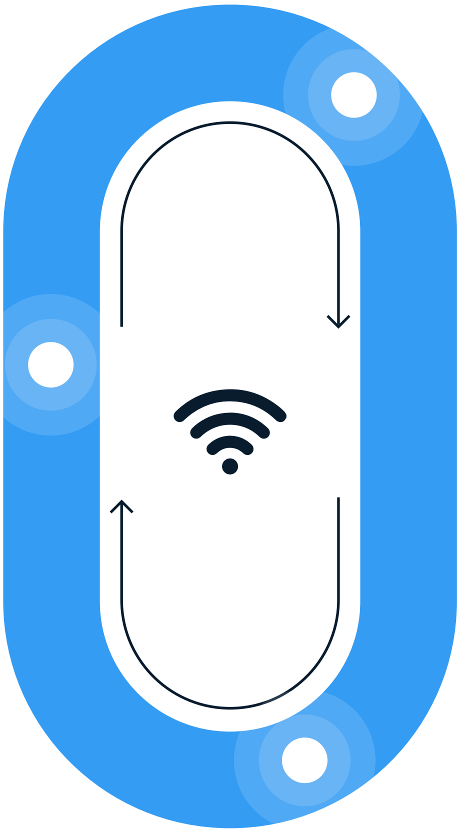
Retailers become early users of IoT because of changes in the market landscape and cost factors. Many retailers, like Tiffany's, Petco, Walmart, and Costco, use IoT differently.

Most sensors will be stationary in stores for an extended period.

Reducing overhead

Today, IoT devices deployed for retail and factory automation must perform multiple calculations on their hardware. These include updating firmware, using GPS, and sending critical system logs. IoT vendors continue to innovate new methods to minimize the need for these tasks to be performed on the edge computing device itself to conserve power and prolong the life of the device.

The IoT market is multiplying, and companies are finding new applications daily. Hardware designers must continually improve existing designs. They must ensure the sensor can run reliably and withstand harsh environmental factors such as extreme temperatures and high humidity.



Common Operating Systems for IoT Devices

Raspbian

The Raspberry Pi is a low-cost, credit-card-sized computer plugged into a computer monitor or TV and uses a standard keyboard and mouse.

Ubuntu Core

Several IoT vendors rely on Ubuntu for their devices, from drones and robots to edge gateways and development boards. They certify their devices to offer users the guarantee of a stable, secure and optimized Ubuntu, either pre-loaded or as a build-your-own option.

OSMC

OSMC (Open Source Media Center) is a free and open-source media player based on Linux. Founded in 2014, OSMC lets you play back media from your local network, attached storage, and the Internet. OSMC is the leading media center in feature set and community-based on the Kodi project.

[Debian](#)

Debian, also known as Debian GNU/Linux, is a Linux distribution composed of free and open-source software developed by the community-supported Debian Project.

[Tizen](#)

Tizen is a Linux-based mobile operating system backed by the Linux Foundation, mainly developed and used primarily by Samsung Electronics.

[CentOS 7.7, 8.2](#)

The CentOS Linux distribution is a stable, predictable, manageable, and reproducible platform derived from the sources of Red Hat Enterprise Linux (RHEL)

[Yocto Linux](#)

The Yocto Project (YP) is an open-source collaboration project that helps developers create custom Linux-based systems regardless of the hardware architecture.

[AWS IoT Greengrass Core devices](#)

AWS IoT Greengrass makes it easy to bring intelligence to edge devices, such as anomaly detection in precision agriculture or powering autonomous devices.

[AWS Linux 2](#)

Amazon Linux 2 is a Linux operating system from Amazon Web Services (AWS). It provides a security-focused, stable, high-performance execution environment to develop and run cloud applications.

Best Practices for IoT Compliance

Achieving a high level of security and compliance for IoT is possible. Best practices embody **five essential steps**:

01

Schedule context-aware updates

IoT upgrades, critical for security, have always meant downtime and delay. Waiting for an update window lets insecure IoT devices remain in service. KernelCare/IoT live-patching offers a solution by automating the update and applying it to a running kernel. Additionally, the KernelCare/IoT initial installation can be done on running devices while they are in service.

02

Set up encrypted communication channels

Communications between the IoT admins and the devices in the field need to be encrypted. While this may sound like an obvious countermeasure, it is common for IoT admin and security work to be conducted in the clear.

03

Develop an adaptable IoT network

All elements of the IoT network must scale as a whole. Automation is critical to attaining this goal. If it breaks down, it will cause IoT services to slow down or fail.

04

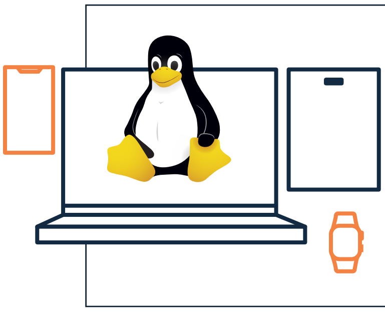
Use firewalls

Although IoT networks are usually outside the leading corporate network, organizations should still set up firewalls to protect sensitive segments of the IoT network. KernelCare/IoT subscribers who require a dedicated patch server inside a secure firewall environment can receive help in setting up our ePortal to administer it.

05

Anticipate consumers' roles and use cases

An organization's customers may use IoT devices differently than initially planned. For example, a user might install Wi-Fi components on the device, leading to an incompatibility with the device updating process.



Organizations prefer IoT devices running standardized operating systems like Linux over devices running custom in-house developed operating systems. This increases the likelihood of security fixes being available when needed.

Patching the OS kernel without rebooting - critical for the IoT market

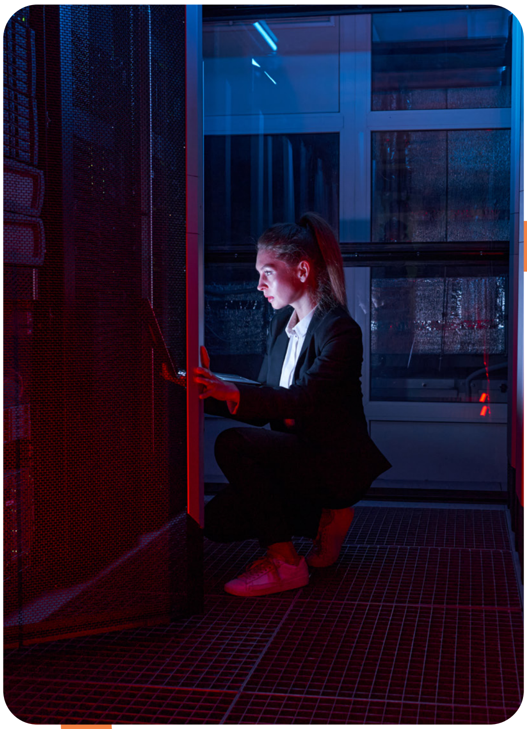
Keep IoT devices secure even if the original vendor is slow to provide patches or does not provide them.

IoT devices enable remarkable efficiency and unprecedented data collection. A tiny unpatched IoT sensor exposes the business to risk as a large-scale server in the data center. It can wreak havoc on information systems or serve as a gateway for malicious actors. Cybersecurity countermeasures are available with KernelCare IoT service embedded devices.

Live patching is deploying patches to a Linux kernel while the device is still running, updating it automatically. It’s rebootless and can be fully automated.

Conclusion

The IoT must be kept secure for its own sake and to protect the organization's digital assets. The challenge is to install much-needed patches to IoT devices without interruptions and downtime associated with rebooting. KernelCare IoT enables admins to use live-patching systems to patch Linux kernels in IoT devices on both Intel and arm chip architectures without interrupting the ongoing processes of embedded devices.



Why TuxCare?

TuxCare team came a long way from the first release of our first service – KernelCare – six years ago. Based on customer demand, we kept adding integrations to vulnerability scanners, reporting and automation tools, and an improved ePortal called KernelCare Enterprise.

Our solutions protect your Linux systems by:

✓ Live patching reduces the window because patches can be applied since there is no need to wait for reboots or service restarts.

✓ The automation portal provides the window because IT teams can reduce the time it takes them to take new patches through staging and testing, then apply them.

✓ The velocity at which our team builds and releases patches for End of Life distributions including PHP and Python allows organizations to get access to them and apply them faster.

Empowering Organizations to Stay Secure and Compliant

TuxCare patch management services have delivered patches and bug fixes for various Linux distros for

over 10 years

TuxCare is approaching

over 1 million

in production workloads secured and supported by our services.

We have over

1500 customers

from multiple industries around the world.

TuxCare has patched more than

80,000 vulnerabilities

without reboots over the years.

We have supported more than

40 Linux distributions

We assist clients in maintaining their compliance requirements and regulatory mandates.

Learn more about what TuxCare's PHP End of Lifecycle Support can do for your organization

Culture

While KernelCare has become a beloved brand to reduce security risks. These days we do a lot more than just take care of the kernel; we protect your Linux systems by live patching security vulnerabilities before they become exploited.

When we took a step back and thought about what we do, we made Linux more secure, stable, and reliable at our core. We take care of Linux so organizations can comfortably and affordably use Linux to support environments requiring high cybersecurity, stability, and availability levels.

CONTACT A TUXCARE EXPERT