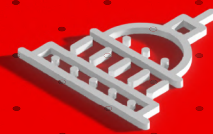




# Security at the edge

A guide to improving  
edge device, application,  
and networking security



# Content

03 — **Introduction**

05 — **Chapter 1**

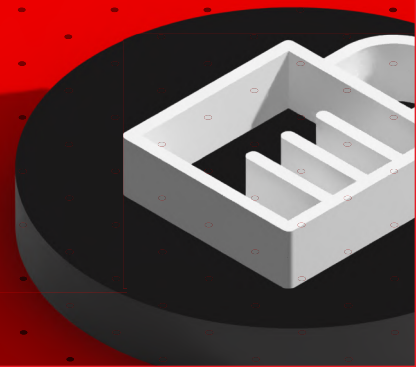
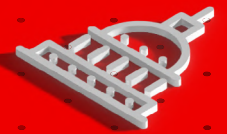
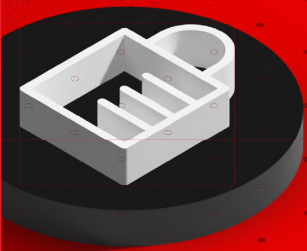
What are the challenges in improving security at the edge?

10 — **Chapter 2**

Best practices to improve edge security

11 — **Chapter 3**

Red Hat's approach to edge security



# Introduction

## Being security-focused isn't easy

Today's global organizations are not limited by geography or borders. The same goes for their infrastructure. Organizations need to deploy applications and infrastructure wherever their business needs dictate. Whether collecting data on a factory floor, processing payments in a retail store, or managing an oil rig in the Gulf of Mexico, meeting customer demands means moving data and processing from the datacenter to where business happens—at the edge.

**70%** of organizations named security as one of the most important factors in edge investments (leading all other factors).<sup>1</sup>

But moving data collection and computing from secure and physically accessible locations like a corporate datacenter introduces new security risks and challenges for organizations.

**As with any security topic, there are no simple answers.**

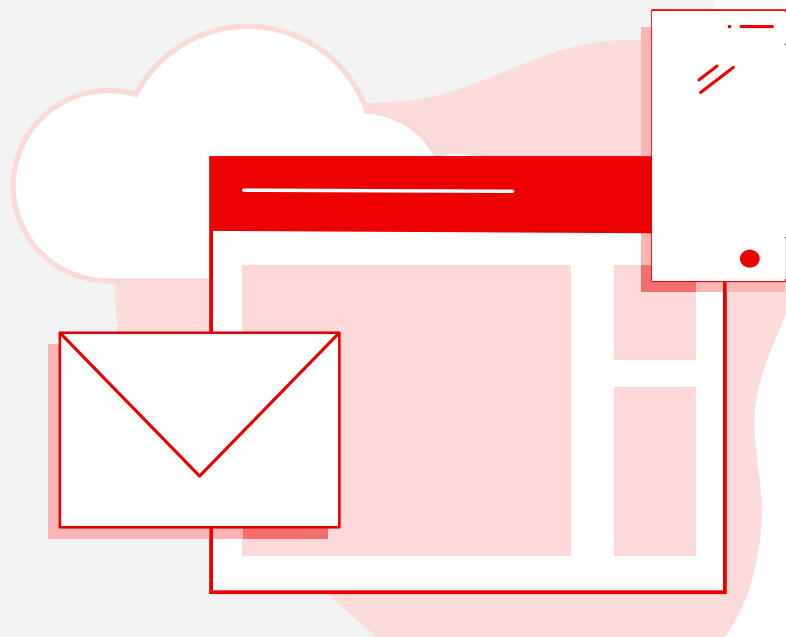
<sup>1</sup> IDC, "Securing the Edge: How Edge Is Architected Will Determine How Security Is Designed." Document #US48547722, Feb. 2022.

Cybersecurity and NetOps professionals must fulfill baseline requirements such as application and information security, authentication and access control, and system updates, and then also address the challenges of securing the edge. These challenges include intermittent internet connectivity, access to edge sites, and internet of things (IoT) edge device security.



Organizations must adapt and evolve the security tools, policies, and processes from their core datacenter or cloud infrastructure to the edge to make edge security work. This is critical to ensure that organizations maintain a strong security posture, governance, and compliance.

Security teams need to have the tools and resources to manage everything from ensuring software is updated consistently to providing security teams with the resources to predict, detect, and address risks proactively—all with the uncertainty of intermittent network connectivity to remote edge locations.





# What are the challenges in improving security at the edge?

In a typical datacenter, it's easy for a network engineer or systems administrator to perform a physical reboot, replace a malfunctioning unit, or apply necessary security updates. Your administrators, DevOps engineers, or site reliability engineers can manage similar tasks with cloud infrastructure.

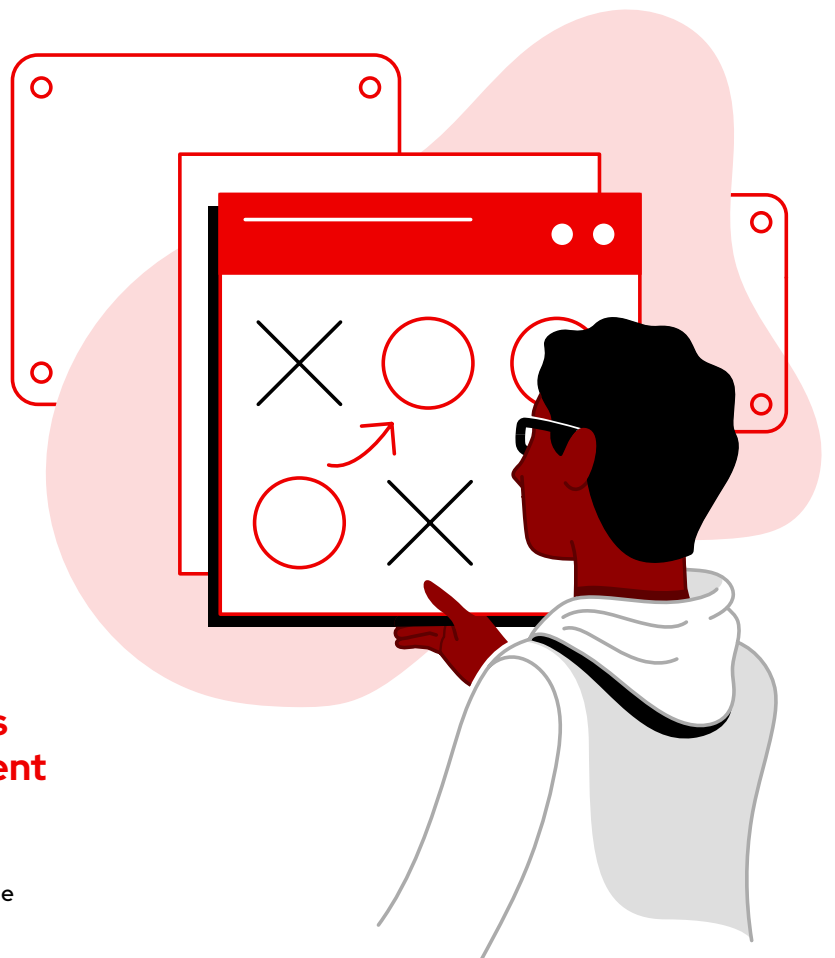
Now consider managing edge devices in retail stores. You may have someone there who can reboot a device, but they cannot apply a security patch or intervene if a security incident or breach occurs. If a device is stolen, the corporate office may only find out about it days or weeks later, increasing the risk of data being retrieved by bad actors.

Computing at the edge often involves legacy software and hardware that adds additional complexity to security policies and processes. Many of these systems run on older operating systems that no longer receive security updates or patches.

**The scale of edge deployments also creates a need for consistent enterprise automation.**

Organizations need to continuously analyze their edge environments to keep track of edge devices, predict security risks, and recommend actions.

**The challenges with extending security to the edge vary by industry, solution, and location.**



Here are five challenges to consider when designing your approach to securing the edge.

# 1.

## Limited or intermittent network access

Collecting and processing data at remote sites is one of the edge's most significant advantages and one of its major potential failure points. Far edge deployments at oil rigs, gas pumping stations, or other remote facilities can have poor or intermittent internet connectivity. This can make it difficult to consistently and reliably download patches and updates to edge devices.

Another challenge of losing connectivity to edge devices is the risk that the device was tampered with while offline. If an edge device is disconnected, it may require physical intervention to reconnect to the network. Still, these reconnections are often done by non-IT employees on retail or factory floors. When those devices come back online, you may need to quarantine them from network resources until verifying their security posture.

Rotation of certificate keys is another important consideration. Imagine you have an edge site where connectivity is only available on specific days during the month. If your scheduled certificate rotation falls on the day that site is offline, you could lose connectivity to that device. Losing connectivity could mean sending an engineer on site to manually update the edge device since it is no longer a trusted device.



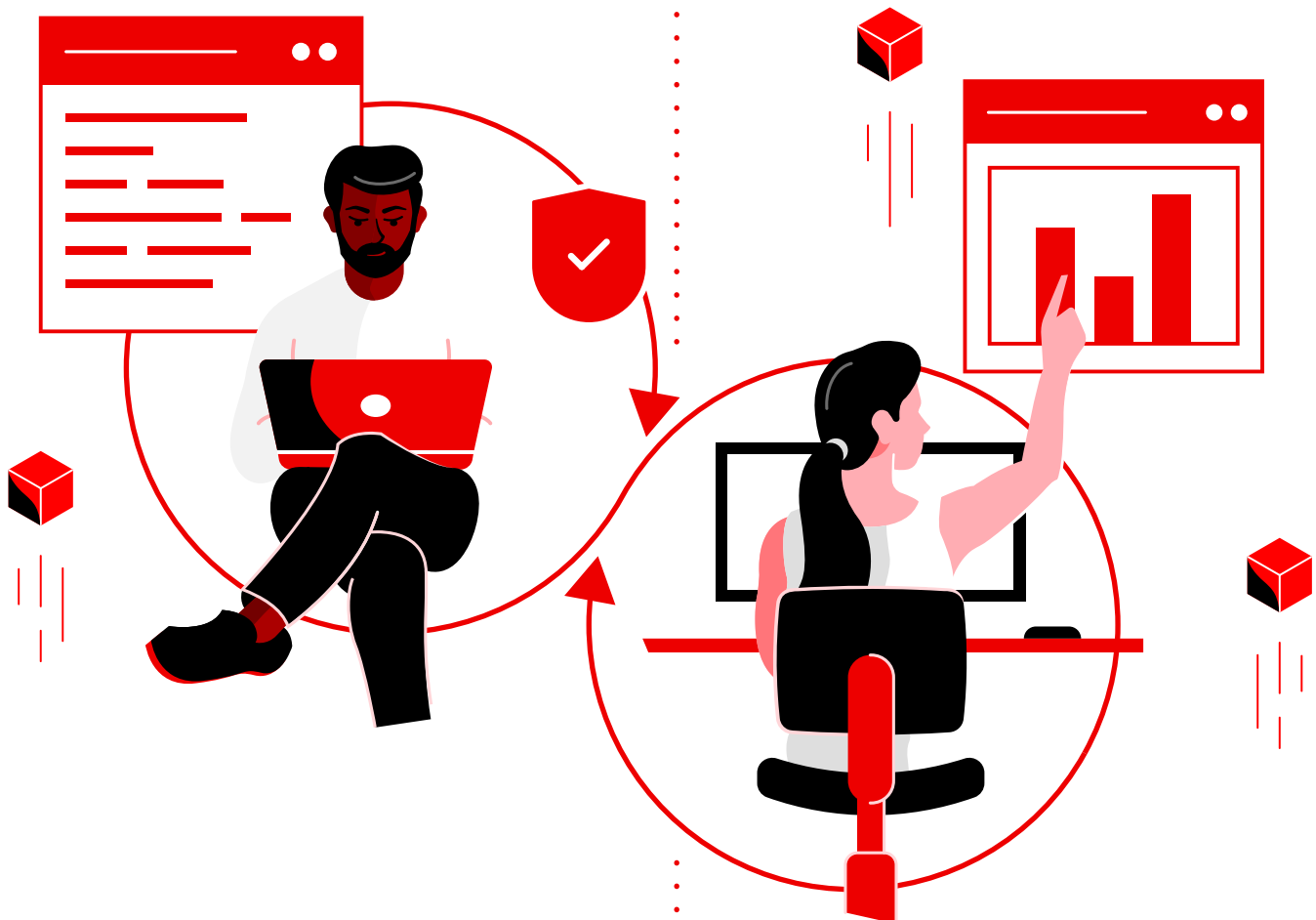
# 2.

## Physical tampering and attacks

The number of devices deployed by an organization at the edge can be in the hundreds to the thousands, often from disparate vendors. One of the first attack vectors at the edge is compromised devices.

Once a compromised device is installed, it can open up additional attack vectors. Due to the remote nature of edge environments, it's not always possible to guarantee the physical security of a device at an edge location. Using edge devices opens up the potential for bad actors to compromise the device via a USB dongle or other attack vectors. These compromised devices could potentially be used to provide backdoor access to a corporate network or other edge devices or applications.

Edge locations can also often be unstaffed for long periods. Without proper security, edge devices can be stolen, creating new security risks. If a device is stolen, sensitive information, including private keys for network access or customer and business data, could potentially be exposed to cyber criminals.

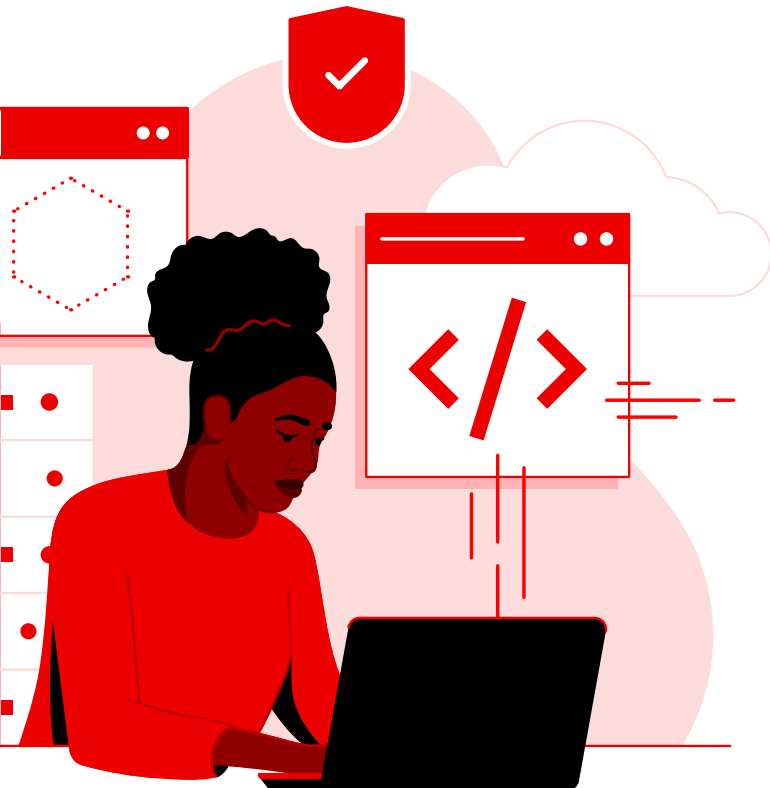
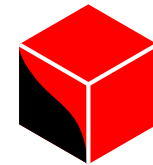
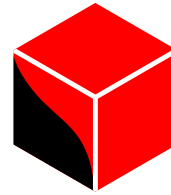


# 3.

## Challenges with edge device remote management

You can easily send an employee to reboot a device or apply an update with on-site datacenters. In the cloud, system administrators or DevOps teams manage these processes. At the edge, there is often no one on-site to reset edge devices if a reboot is required or to address other security issues.

Between edge environments being physically distant and often having poor or nonexistent connectivity, one of the most significant challenges with remote management is the application of patches and updates for edge devices. These are more than security updates for the device operating system. Organizations must consider the entire device stack, including the device's basic input/output system (BIOS), operating system (OS), WiFi or cellular stack, and any applications.



# 4.

## Preventing traffic interception at the edge

Beyond the issue of limited or intermittent network connectivity, edge devices can also present bad actors with opportunities to intercept network traffic. This traffic can include customer or business data, Secure Sockets Layer (SSL) and Secure Shell Protocol (SSH) keys, or other data that can open your central infrastructure to further attacks.

Increasing security around WiFi connectivity at the edge is another challenge. From the edge devices to WiFi access points, organizations have to ensure that WiFi radio patches are applied, and access point service set identifiers (SSIDs) are rotated frequently to reduce the potential for bad actors to infiltrate corporate networks through poorly secured edge WiFi networks.



# 5.

## Preventing human error in edge security

As with any conversation around security, the weakest link in edge security is people. According to the 2022 Verizon Data Breach Investigations Report, 82% of breaches involved human attack vectors such as social attacks, errors, and misuse.<sup>2</sup> Many edge locations are not staffed with IT or networking specialists. This introduces numerous potential attack vectors, from lax login credential security, to even leaving manufacturer default passwords on edge devices to make it faster to restart devices when necessary.

Additionally, staff at edge locations often rely on “shadow IT”—the use of devices, applications, or tools that are not approved by an organization’s IT or security operations teams. This use of uncontrolled or unmanaged technologies, creates additional attack vectors within an already at-risk infrastructure.

**82%** of breaches involved human attack vectors.<sup>2</sup>



**The lightweight and mobile nature of edge and other IoT devices poses a perception problem at these locations. Employees can perceive the devices as not being critical parts of the infrastructure, exposing them to tampering or theft.**



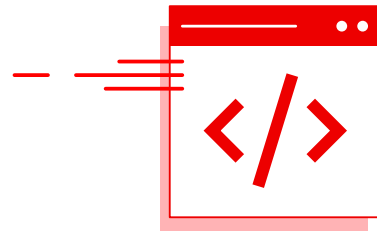
<sup>2</sup>Verizon, “2022 Data Breach Investigations Report,” 25 May 2022.

# Best practices to

# improve edge security

## Automate management of edge hardware and firmware

Edge devices can often be the first attack vector. Reduce the risks by using automation tools to ensure device patches, such as boot ROM, and device firmware are applied, in an automated and consistent way, regardless of limited or intermittent network connectivity. If possible, use physical barriers to restrict access to devices to prevent tampering through USB or other ports.



## Reduce human errors with automated device onboarding and provisioning

Zero-touch provisioning allows for edge devices to be provisioned in a network automatically, freeing system administrators to perform specialized tasks and reducing human errors by eliminating required manual configuration efforts, downtime, and travel time to physical sites. Additionally, zero-touch provisioning can be performed at scale and much more rapidly, which are all key to doing edge security at scale.

## Integrate security throughout the application life cycle

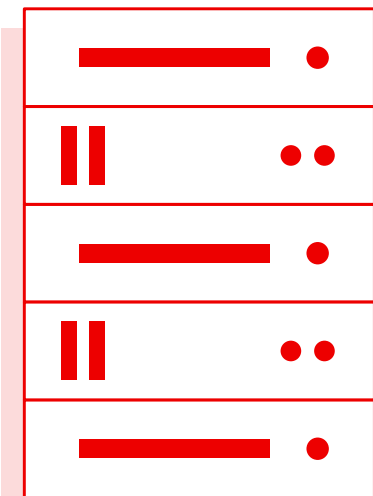
Edge security involves more than the device. Applications running on any device need continuous security at every stage of the application development life cycle. This includes development and build, deployment, and runtime. In addition, audit, monitoring, and logging should be in place so that you can be notified of and log key security incidents after the applications are deployed and running in production environments to remediate accordingly.

## Encrypt network security end to end

Edge devices have a high potential to be compromised. Organizations should consider segmenting their networks and using policy-based decryption (PBD) to better control network traffic and secure sensitive data in transit for improved security. Automation and monitoring tools should also be employed to analyze networks for suspicious traffic activity and remediate issues accordingly in an automated fashion at scale.

# Red Hat's approach to edge security

Red Hat's open-source edge computing solutions can help organizations streamline operations and improve security across edge environments through automated provisioning and hardening, management, predefined configurations, and orchestration.



## Deploy at the edge with a stable foundation

"Red Hat offers the right combination of people and products to address our business and technical challenges, including a roadmap to edge computing."<sup>3</sup>

### IDF lieutenant colonel

Head of Edge Cloud Platform R&D, Mamram, C4i and Cyber Defense Directorate.



Edge projects introduce multiple challenges, from verifying hardware is not compromised to addressing remote management issues. Having a stable foundation is critical to edge data collection and computing. Red Hat® Enterprise Linux® helps organizations to deploy mini server rooms on lightweight hardware at the edge for consistent and hardened operating environments. It's built for workloads requiring long-term stability and security services on certified hardware, software, cloud, and service providers.

<sup>3</sup> Red Hat. "Israel Defense Forces' IT unit delivers as-a-Service capabilities faster with Red Hat." 26 April 2022.

## Manage complexity at the edge

Edge projects can include hundreds or thousands of edge devices, creating numerous security challenges for organizations. These include ensuring devices have the correct security patches and managing device inventories for missing or potentially stolen devices.

Red Hat Ansible® Automation Platform provides on-premise, cloud, hybrid cloud, and edge automation capabilities. It also provides organizations with a common automation language from development to production that supports third-party solutions and content. Consistent enterprise automation is critical to keeping environments up to date and fixing security issues on edge devices at scale.



“The massive addressable domain of in-vehicle and edge software in modern vehicles necessitates an ecosystem-driven approach to reduce software development costs for automakers, nearly half of which is dedicated towards maintenance and triage. At the same time, maintaining strict compliance with safety standards mandates high levels of assurance in the underlying software.”<sup>4</sup>

**Alex Oyler**

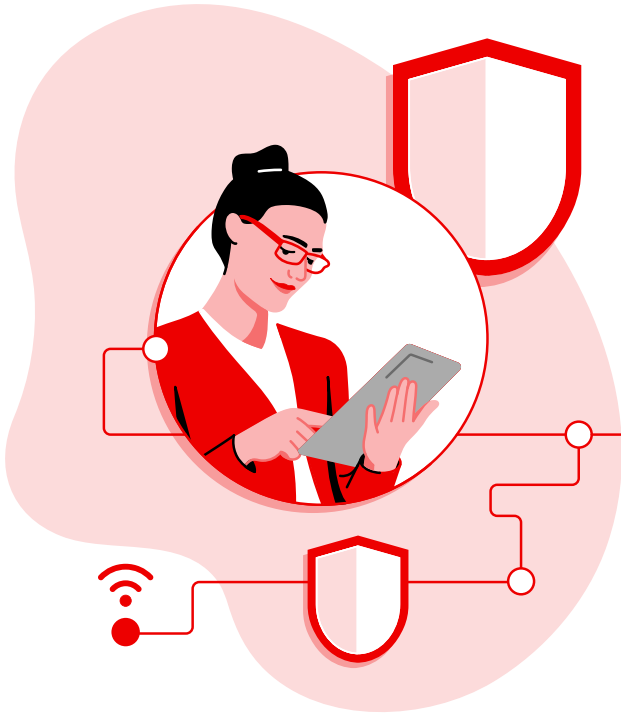
Director, North America, SBD Automotive

<sup>4</sup>Red Hat press release. [“Red Hat and General Motors Collaborate to Trailblaze the Future of Software-Defined Vehicles,”](#) 10 May 2022.

## Monitor the edge 24x7

Having a strong foundation for security only works if organizations continuously analyze their edge environments to predict risk and recommend actions.

Red Hat Insights monitors Red Hat Enterprise Linux systems at the edge for vulnerabilities, configuration issues, and other potential security issues and can generate Ansible Playbooks, which can be used to remediate risks at scale. Edge environments can also be monitored and managed with security information and event management (SIEM) or security orchestration automation and response (SOAR) tools from partner providers. Ansible Automation Platform Certified Content collections are available to provide certified Ansible automation content that integrates with and supports SIEM, SOAR, endpoint protection and other third-party solutions.<sup>5</sup>



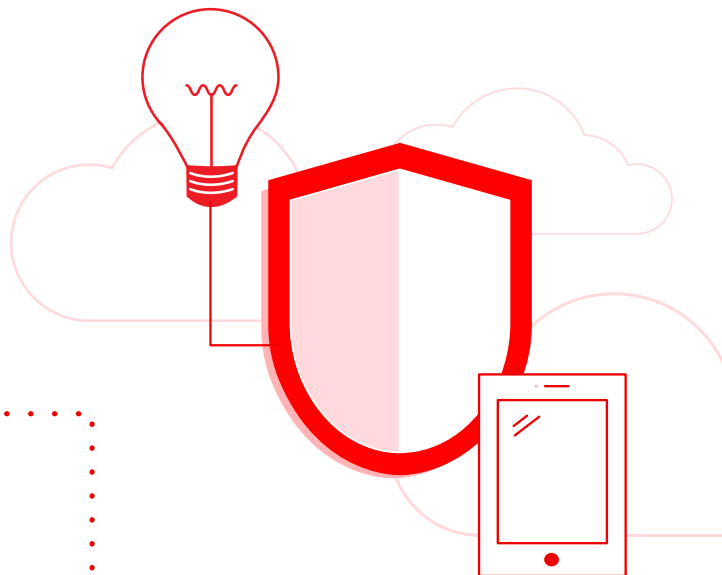
## Boost security for both traditional and containerized environments

The same edge security issues that affect device management can make it challenging to build, deploy, run, and manage container-based applications on edge devices. Red Hat OpenShift® is a Kubernetes platform that provides granular access control, auditing, logging, and monitoring capabilities for containerized workloads running in Red Hat OpenShift and can be used to provide end-to-end encryption for edge device communication.



<sup>5</sup> Red Hat. "Ansible Automation Platform Certified Content," Red Hat Customer Portal, 28 July 2022.

Organizations can also use Red Hat Advanced Cluster Management for Kubernetes, Ansible Automation Platform, and Red Hat Insights to identify and respond to security risks. Red Hat technologies provides robust built-in policy and compliance capabilities for compliance to industry standard security frameworks, including Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Security Standards Council (PCI), and more for both traditional and containerized environments.



In addition, Red Hat Advanced Cluster Security for Kubernetes and Red Hat OpenShift help organizations to automate their DevSecOps workflows for container-based applications and protect these applications deployed at the edge across the complete application life cycle: from build to deploy to run.

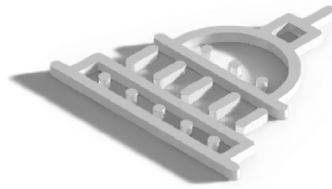
## Learn more

### Ready to boost your edge security?

Red Hat has the solutions and the expertise to help bring your security from the datacenter to the edge.

- Discover [Red Hat's approach to hybrid cloud security](#).
- Learn more about [Red Hat Enterprise Linux security and compliance](#).
- Start your trial of [Red Hat Ansible Automation Platform](#) and [Red Hat OpenShift](#).





facebook.com/redhatinc  
@redhat  
linkedin.com/company/red-hat

### About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers develop cloud-native applications, integrate existing and new IT applications, and automate and manage complex environments. A trusted adviser to the Fortune 500, Red Hat provides award-winning support, training, and consulting services that bring the benefits of open innovation to any industry. Red Hat is a connective hub in a global network of enterprises, partners, and communities, helping organizations grow, transform, and prepare for the digital future.

**North America**  
1 888 REDHAT1  
www.redhat.com

**Europe, Middle East,  
and Africa**  
00800 7334 2835  
europe@redhat.com

**Asia Pacific**  
+65 6490 4200  
apac@redhat.com

**Latin America**  
+54 11 4329 7300  
info-latam@redhat.com

redhat.com

Copyright © 2022 Red Hat, Inc. Red Hat, the Red Hat logo, OpenShift, and Ansible are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.