Modernize edge computing in oil and gas with Red Hat and Intel

Introduction

Edge computing pushes processing to the edge of the network—close to the location where data is created and collected. As this relatively new computing model gains momentum, industry analysts predict that edge computing will exceed 37% compound annual growth rate (CAGR) from 2020 to 2027.[1] However, the oil and gas industry has been operating at the edge for decades. Supervisory Control and Data Acquisition (SCADA), which originated in the energy and mining fields, was actually the precursor of the Industrial Internet of Things (IIoT).

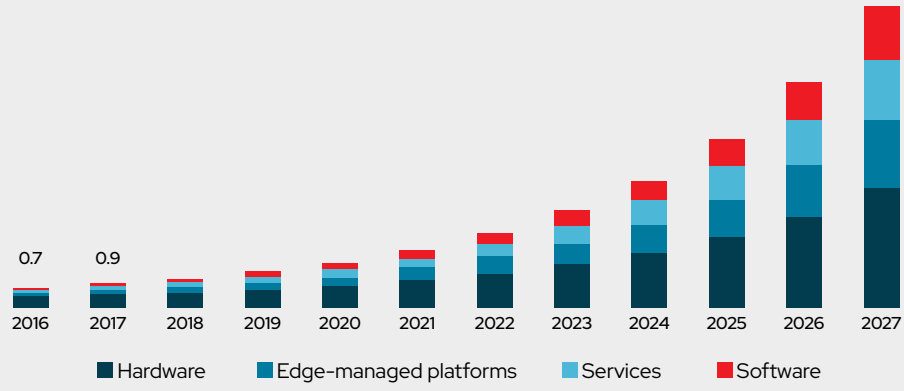

Figure 1. U.S. edge computing market size by component (in USD billion)[1]

This paper describes how Red Hat and Intel combine leading microprocessor hardware and open source software to address edge computing challenges. This joint effort offers a more secure edge architecture that includes hardware-based security and other device features, an open enterprise operating system (OS), container management, and automation. With a new model based on industry-standard edge hardware and open source software, oil and gas companies can reduce costs and complexity and improve security.

Red Hat Enterprise Linux 8.3 complements other Red Hat open software solutions to mitigate a number of business and technical risks associated with edge computing:

- Stored data lacks the physical security protections typically found in datacenters.
- An expanded IT perimeter complicates perimeter defense overall.
- Updating and validating edge device security can be difficult without on-site visits.

It also helps to remove network blockers that result from a culture of segmented data—that is, "my data, not your data."

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

1 *Grand View Research. "Edge Computing Market Size, Share & Trends Analysis Report by Component (Hardware, Software, Services, Edge-managed Platforms), By Industry Vertical (Healthcare, Agriculture), by Region, and Segment Forecasts, 2020 – 2027," Grand View Research, March 2020.*

Opportunity

By monitoring real-time data everywhere from the borehole to the pipeline to the downstream facility, SCADA can tell operators the performance of drilling, delivery, and process equipment. It also controls various processes remotely. This broadly deployed industrial monitoring and control system has become essential to the safety and efficiency of energy industry operations.

For example, used in combination with seismic tools on a ship or truck, telemetry collected in the field can determine the type of subsurface formation before drilling. If it is bedrock or other material that could damage the drill, the operator (or the system) can adjust the drill speed accordingly. Over time, the remote sensors and control equipment have become more connected and more capable of processing data.

With today's IIoT devices collecting huge volumes of data and incorporating greater processing power, the traditional SCADA model has evolved into what we now call edge computing. Rather than burdening network bandwidth by transferring large volumes of raw data back for analysis, small footprint compute devices process the data at the edge of the network, sending back only results or alerts. This approach reduces data gravity—that is, it makes it faster and less costly to backhaul data to a cloud or datacenter.

Edge computing forms an efficient bridge between the devices and the cloud or datacenter "edge." However, calling it the edge is somewhat of a misnomer because it actually does not matter where the data processing happens—i.e., it is location-less. For example, the typical resource-constrained edge device currently cannot run an enterprise-grade operating system. But near-edge gateways can, and this is still commonly referred to as edge computing.

Challenges at the edge of the network

Moving computing out of the datacenter or cloud and closer to the origin of data presents challenges:

- How do you manage these edge computing systems at scale—moving from hundreds to perhaps hundreds of thousands or even millions of devices?
- How do you know that an edge device is still there or that it is connected?
- If a vulnerability surfaces for the device, how will you patch it?
- How do you push new applications to a device?
- How do you ensure interoperability in multivendor and heterogenous software environments?
- How do you ensure that edge devices are deployed, managed, and updated in a consistent and secure way?

In general, all of these challenges revolve around security since edge computing moves data beyond the safety of the datacenter.

As oil and gas companies modernize their IT infrastructures, many also want to repurpose and derive data value from existing operational technology (OT) deployments. For example, they may want to develop a new edge computing architecture that interfaces with existing SCADA deployments in onshore and offshore settings, which may be collecting millions of SCADA tags in a single day.

The joint edge computing solution from Red Hat and Intel helps oil and gas companies understand how to modernize their IT infrastructure while protecting growing volumes of data collected at the edge. This approach can help energy companies determine if they should buy or build a modern edge computing environment. For example, an oil company may want to buy an architecture to avoid multiple end-to-end solutions and closed proprietary systems. The security weakness common to some end-to-end solutions can lead to serious risks, such as a compromised edge device allowing an attacker to access public cloud credentials.

As an alternative, the company may choose to buy the IIoT sensors and actuators at the edge of the network from various players in the market. Then, they can define an architecture that provides a comprehensive view of the security of the implementations in the field. The solution developed by Red Hat and Intel enables this option because it is based on open software and industry standards.

How Red Hat helps to more securely scale edge computing

Red Hat® Enterprise Linux® 8.3 complements other Red Hat open software solutions to mitigate a number of business and technical risks associated with edge computing, such as:

- Stored data lacks the physical security protections typically found in datacenters.
- An expanded IT perimeter complicates perimeter defense overall.
- Updating and validating edge device security can be difficult without on-site visits.

It also helps to remove network blockers that result from a culture of segmented data—that is, "my data, not your data."

Red Hat Enterprise Linux

Red Hat Enterprise Linux is the world's leading enterprise Linux platform.[2] This open source operating system forms the foundation for today's hybrid cloud environments, offering a number of benefits, such as the freedom and flexibility to more securely run workloads where they are needed. In addition, users can scale existing apps and roll out emerging technologies—across bare metal, virtual, container, and all types of cloud environments. Red Hat Enterprise Linux 8.3 includes a new edge deployment option, solving a number of the challenges common for edge environments (Fig. 2).

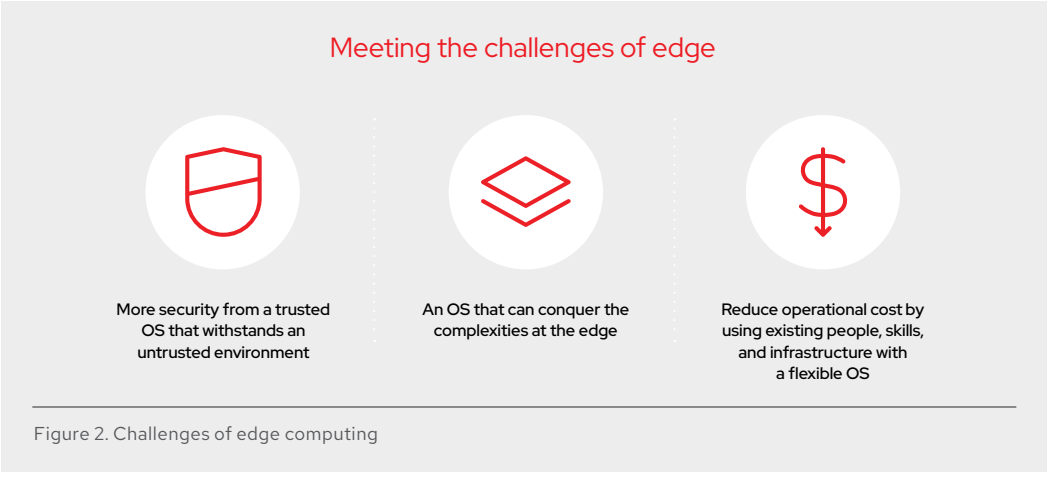

Figure 2. Challenges of edge computing

2 *Worldwide Operating Systems and Subsystems Market Shares, 2018; released November 2019.*

Application isolation benefits security and operational concerns

Applications deployed on Red Hat Enterprise Linux can be isolated from the operating system via Open Container Initiative (OCI) containers. These containers use low-level OS primitives to create a sandbox that greatly limits the surface area of the underlying operating system. From a security perspective, this feature makes it much simpler for applications to have a better security posture by default. On the operational side, decoupling applications from the underlying operating system means they can be maintained, patched, and managed independently. Separating application deployment via containers creates the opportunity to adapt systems in the field that were historically static. Oil and gas users can benefit from both the OS's enterprise life cycle and increased flexibility to maximize the longevity and usefulness of their edge systems.

Fast image assembly and consolidation

The image builder tool in Red Hat Enterprise Linux provides a versatile solution for configuring and creating custom system images. It allows developers to quickly spin up new Red Hat Enterprise Linux systems in a variety of cloud and virtualization platforms. Image builder provides a streamlined interface to configure purpose-built Red Hat Enterprise Linux images that meet workload requirements and accelerate device provisioning at the edge of the network.

Transactional updates with intelligent rollbacks

Red Hat Enterprise Linux uses a technology called rpm-ostree to provide a native A/B-image-style update mechanism, also known as transactional updates. This feature dramatically improves the resilience of OS updates and ensures nodes always maintain a "known-good" state. It also requires less time to mirror updates created with image builder for edge systems to stage and apply updates during maintenance windows. This workflow greatly simplifies the act of patching systems or individual packages in the field.

Greenboot is a new capability that connects application-specific healthchecks with the rpm-ostree update mechanism. If an issue affects an application, the system will automatically roll back changes and preserve the working state. This feature helps to eliminate having to choose between application stability and staying current on OS security updates.

Red Hat Enterprise Linux, through the inclusion of rpm-ostree and greenboot, can reduce or even eliminate the need for rolling trucks. It can also improve edge service-level agreements (SLAs) for connected or lights-out deployments (a computing environment that can operate with minimal human involvement).

Delta security updates

The update payloads for rpm-ostree are highly optimized for intermittent and low-bandwidth connections, transferring only a fraction of the data used by a traditional package-based distribution. This feature is particularly beneficial for sites where network bandwidth is limited, as it helps preserve the available network bandwidth for other consumers and applications.

Commercially supported open software

Compared to free versions, commercially supported open source software provides business benefits such as a single source for support and updates. Open source software also speeds innovation with access to the global open source developer community. You can also work more efficiently with hardware and software partners and typically interact directly with the engineers that can address issues and create working solutions for the market.

Other benefits of Red Hat software for edge computing

Red Hat software provides everything needed to automate and manage infrastructure—from your core datacenter to your remote edge sites. Red Hat OpenShift® provides more secure orchestration of Kubernetes containers. It allows you to deploy and manage container-based applications across any infrastructure or cloud—including private and public clouds or edge locations.

Red Hat Ansible® Automation Platform can be used to programmatically manipulate every layer of a computing architecture—from orchestration to deployment to configuration. In this way, oil and gas companies can use Ansible Automation Platform to automate edge infrastructures.

The security hardening features built into Red Hat Enterprise Linux and Red Hat OpenShift can also help reduce overall risk for edge computing. Plus, they mitigate compliance risk by preparing customers for additional federal legislation on IoT security coming in the Health Insurance Portability and Accountability Act (HIPAA) and the Cybersecurity Vulnerability Remediation Act. It also addresses similar guidance from the National Institute of Standards and Technology's (NIST's) IoT Device Cybersecurity Capability Core Baseline and the Cloud Security Alliance (CSA) IoT Working Group.

Intel provides the foundation for Red Hat edge software solutions

The cooperation between Red Hat and Intel helps to bridge current technology enablement gaps that exist in oil and gas edge computing and IT infrastructure. In addition to the security provided by Red Hat solutions, open source software is inherently more secure as it is more transparent. Your IT team can see the code, which means they can examine it for security flaws rather than relying on a proprietary software vendor to assess security. The large open source community can also see the source code, and the more eyes on the software, the fewer bugs in the code.

The combination of Red Hat open source software running on Intel hardware offers a solution with hardened security that protects data at rest, in transit, and in use.

A number of capabilities underpin the security of this edge computing environment.

Secure Boot

Secure Boot has become an industry standard because the technology provides a number of strengths. It delivers a framework in which the firmware verifies that the system's boot-loader, kernel, and potentially, user space are signed with a cryptographic key authorized by a database stored in the firmware. It relies on cryptographic signatures that are embedded into files using the Authenticode file format. The integrity of the executable is verified by checking the 6 hash. Finally, the authenticity and trust is established by checking the signature, and the signature is based on X.509 certificates and must be trusted by the platform.

Data encryption

Data encryption protects the private data stored on each of the hosts in the IoT infrastructure. The Linux Unified Key Setup (LUKS) is the standard for Linux hard disk encryption. By providing a standard on-disk format, it facilitates compatibility among different distributions and more secure management of multiple encryption keys.

By using the Trusted Platform Module (TPM) 2.0 as credential storage for disk encryption keys, Intel mitigates the security risk of having disk encryption keys stored in plain text on the device disk. This approach also eliminates the need to distribute keys through an insecure channel where they could be disclosed.

Execution policies and integrity protection

The Intel solutions fulfill the goals of execution policies and integrity protection in a number of ways. They detect if files have been accidentally or maliciously altered, both remotely and locally. The solutions also appraise a file's measurement against a "good" value stored as an extended attribute. In addition, they enforce local file integrity—based on goals complementary to the Mandatory Access Control (MAC) protections provided by Linux Security Modules (LSM), such as Security-Enhanced Linux (SELinux) and Smack. Depending on the policies that administrators establish, these modules can also protect file integrity (including appraisal hash) against off-line attack.

Components

Based on the Trusted Computing Group's open standards, Integrity Measurement Architecture (IMA) measurement comprises a key component of the Linux kernel's integrity subsystem. As part of the overall IMA, measurement maintains a runtime measurement list and, if anchored in a hardware TPM, delivers an aggregate integrity value over this list.

The benefit of anchoring the aggregate integrity value in the TPM is that the measurement list cannot be compromised by any software attack without being detectable. IMA measurement can be used to attest to the system's runtime integrity. Based on these measurements, a remote party can detect whether critical system files have been modified or if malicious software has been executed.

Credentials

For credentials, Intel uses an approach that generates strong cryptographic keys derived from source and large key space. The private key material never leaves the TPM secure boundary in plain form. The TPM stores keys on one of four hierarchies: endorsement, platform, owner (also known as storage), and null.

Data sanitization

Data sanitization assures confidentiality by rendering access to target data—the data subject to the sanitization technique—on the media infeasible for a given level of recovery effort. The level of effort required may range widely. For example, a hacker might attempt simple keyboard attacks without the use of specialized tools, skills, or knowledge of the medium's characteristics. Or, bad actors might apply state-of-the-art laboratory techniques in their attempts to retrieve data.

Intel implements effective data sanitization using the cryptographic erase (CE) process, which is widely used in self-encrypting drives. This technique leaves only the ciphertext remaining on the media, effectively sanitizing the data by preventing read access. Without the encryption key used to encrypt the target data, the data is unrecoverable. In other words, the encryption itself sanitizes the data.

Case study: How one oil supermajor modernized and added security to its edge computing platform

While cloud computing offers key benefits for many OT workloads, it also presents challenges for edge and IIoT use cases, including:

- Control plane latency.
- Management of massive volumes of remote data.
- Data aggregation.
- Manual management of complex edge stacks due to a lack of manageability standards.
- Security concerns for data and systems located far away from the datacenter.

An oil supermajor approached Red Hat and Intel to help develop and deploy a platform to address some of these challenges. The result was a foundational framework that enables the supermajor to adopt digital technologies for the edge of the network in a scalable and managed way. The framework also provides the security required by the supermajor. Security is a top priority as a cyberattack can cause risk to life or to the safety of employees and people who live near pipelines and production, processing, and storage facilities.

Red Hat's open source software allowed key players in the IIoT space—such as device manufacturers—to contribute to this customer-focused initiative. The Red Hat and Intel collaboration resulted in a framework that can enable any oil and gas company to adopt digital technologies in a scalable, managed, and more secure way.

Intel and Red Hat also worked with the customer's team to implement the tenets of an open, secure, and interoperable process control architecture. This effort aligned with the supermajor's long-term goal of industry innovation. For example, a successful deployment could encourage industry players to work toward open solutions. If vendors incorporate open source technologies in their edge solutions, their customers can take advantage of open source software and open hybrid clouds.

The supermajor's open source foundation provided an ideal starting point for a hybrid cloud approach, which delivered a number of benefits:

- Security
- Scalability
- Application and workload portability
- Resiliency and reliability for edge computing systems

Using Red Hat and Intel technologies, the supermajor built an enterprise-grade architecture to enable digital transformation at scale. It provides both data security and compliance with a global security model that can support any use case or workloads, including protecting sensitive data at rest, in transit, and in use, as well as trustworthiness of the overall system. It also helps the supermajor comply with various privacy regulations while facilitating global expansion. In addition to enabling data sovereignty compliance, the solution makes it possible to operate in countries where governments mandate the use of local public cloud providers—such as Alibaba in China.

About Intel

Intel, a world leader in silicon innovation, develops technologies and initiatives to advance how people work and live. Second-generation Intel Xeon Scalable processors with Intel Optane DC persistent memory form the reference design platform for SAP HANA. It delivers optimal performance, security, flexibility, and total cost of ownership to meet today's data center needs. Make better business decisions faster with an intelligent data management strategy from Intel and SAP.

Additionally, the architecture addresses many of the concerns associated with monitoring, optimizing, and ensuring the reliability of widely dispersed field assets while increasing capital efficiency. For instance, the open approach resulted in not only cost savings but also an environment that helps to avoid vendor lock-in by providing interoperability between edge, cloud, and on-premise environments. This interoperability also makes applications and workloads more portable.

Conclusion

To operate more efficiently, oil and gas companies need to modernize their IT infrastructure, and remote monitoring and control comprises a critical area for improvement. The increased processing and storage of IIoT devices means that more data can be collected and processed at the edge of the network.

Red Hat and Intel have collaborated to develop complementary solutions to make edge and connected hybrid clouds more secure and efficient. Using open standards and open software, the foundation allows oil and gas companies to either augment existing SCADA systems or replace them with a new model consisting of low-cost IIoT devices connected to hybrid clouds. This open approach also provides the flexibility oil and gas companies need to efficiently and cost-effectively modernize their edge computing.

The joint solution addresses a core concern of edge computing in oil and gas—security. For example, gateways at the near-edge running Red Hat Enterprise Linux can process vast amounts of data from IIoT monitoring and control edge devices. Intel adds key security capabilities, such as Secure Boot and data encryption using the TPM 2.0 as credential storage for keys. Consequently, the Red Hat and Intel approach ensures this data is stored, processed, transported, and used with strong security. Essentially, it offers the safety of the datacenter for devices in the wild. The result is an edge device and hybrid cloud architecture that provides a modern foundation with the security required to reap the benefits of edge computing.

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 integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

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

NORTH AMERICA
1 888 REDHAT1

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
#F27063_0221