A Deep Dive on Edge+Security

The emergence of edge computing has been swift and broad across the business technology scene around the world. For enterprises and organizations that are eyeing or using the technology within their own operations, edge computing can make them more agile, more efficient, and better prepared to grow their businesses in the global marketplace.

The rapid proliferation of edge computing has been fueled by the cascading growth of data that is used and located further away from traditional data centers. That includes data that exists in a wide range of places across all aspects of their company's operations. It also includes data growth created through the steady acceleration of industrial IoT device deployments and by other business use cases where enterprises are realizing the value of processing and analyzing their data at the edge of their networks.

Edge computing is one of the fastest growing technology needs in the world today for enterprises of all types and sizes. More companies are finding that mission-critical edge services can help them boost quality and accelerate innovation. But like the broad topic of cloud computing, edge computing can be complicated, difficult to deploy and manage, and requires specific expertise to make it work as a well-oiled part of an organization's vast technology infrastructure.

A critical topic when discussing edge computing is security — how the systems and their vast stores of business-generated data can be kept safe and protected from threat actors. Edge security can be especially vexing because valuable business data is being processed in a much higher volume of remote places far from the traditional security perimeters of previous security strategies.

Such security concerns for edge computing deployments require consideration from their inception. As companies begin seeing the benefits of the edge and artificial intelligence technologies they will also likely want to increase their usage to accelerate innovation, improve the business value, quality and yield of their products and services, while addressing worker safety, sustainability, and a host of other possibilities.

Security Challenges in Edge Computing Deployments

The mandatory requirements for data and system security when using edge computing deployments are one of the greatest challenges when designing, implementing, and using the technology. And security becomes even more critical as the volume of a company's data and edge computing efforts continue to expand. Locked-down security capabilities are must-haves so that enterprises can safely get their valuable business data out to where it is needed, knowing they are protected from data breaches, cyberattacks and other security worries.

These edge computing security challenges and concerns are heard across a wide range of businesses, including telco, shipping, cruise lines, industrial facilities, factories, retail deployments and more, wherever there are satellite locations that are not connected to traditional data center compute facilities. Common challenges we are seeing include:

The security challenges of distributed architecture. IT security is also challenging, but everything is typically within an enterprise's centralized, locked-down infrastructure. With edge computing, those big, thick castle walls are gone, replaced by a vastly different distributed architecture where security can be tougher to ensure. The attack surface areas for potential breaches are vastly expanded in edge computing deployments because they can include physical, network, virtualized, and containerized applications and technologies. And as the number of devices soars as well, the complexity of keeping it all safe becomes much more difficult.

Securing data in motion. And if edge computing's security challenges are already not enough, there are inherent security worries about data that is in motion from one place to the next at the edge. Having to protect data in motion while it is being sent from one place to another brings up its own worries about cyberattacks and the challenges of protection. These worries are in addition to the existing and ever-present concerns about data that is in storage and at rest.

Ensuring overall security of an enterprise's technology infrastructure. While one must immediately lock down the security of their edge computing deployments as early in supply chain and design phases, companies must ensure that the rest of their corporate IT infrastructure is also protected from top to bottom as well. Any vulnerabilities in an organization's core IT infrastructure will provide direct access for attackers to go after the edge computing deployment. Edge deployments increase, not only the volume of devices that are in use, but also the breadth of vendor technologies for hardware, software and operational tooling.

Ensuring that only authorized parties have access to edge computing data. With edge data, organizations need to ensure that it is available to only the users and applications that are authorized to have access. Today's systems and edge computing deployments are better protected by locking all systems down by default and then providing access only to authorized individual users and applications as required, but as more employees work remotely it's critical for organizations to ensure only the right people have access to the right data only as required.

Edge deployments require physical and digital security. In edge computing, both digital and physical security protections must be adopted and in place to assure a complete security framework for enterprises. To protect a company's data and business they need a layered, defense-in-depth security approach that takes advantage of the capabilities of each layer in their environment, from physical hardware to applications, as well as the development, operations and business processes in-between them.

Red Hat's Approach to Security at the Edge

Red Hat provides trusted open source software that helps organizations implement a consistent, layered security approach across their hybrid cloud infrastructure, application stacks, product and business process life cycles. Red Hat takes a zero trust security approach from the foundation of a secure immutable operating system, application platforms, and development tools applied across critical workloads for tight security whether on-premises, in the cloud, or at edge computing sites. Red Hat technologies are developed with a secure software supply chain process so enterprises can build and deploy their applications on a trusted hybrid cloud. As part of this process, Red Hat includes software provenance, image and vulnerability of source code, along with extensive quality assurance and regression testing, hardening, and distribution through a protected channel, providing continuous rapid delivery of security updates for all supported packages included in Red Hat products.

To make this all happen, each time a customer uses a Red Hat product, tool, or deploy third-party applications, Red hat follows a Zero Trust security approach which is based on the premise that every interaction begins in an untrusted state. As part of this approach, Red Hat applies many software platforms and application isolation, authentication, and encryption mechanisms including operating in FIPS trusted mode. This contrasts with traditional architectures which may determine trustworthiness based on whether communication starts inside a firewall. Zero Trust attempts to close gaps in security architectures that rely on implicit trust models and one-time authentication. The Zero Trust model is applied by Red Hat across every one of its platforms, tools, application development environments, managed cloud services as well as third party applications developed and deployed by customers and partners.

These critical security principles are applied across private, public, edge environments from the beginning of the supply chain to development and across testing, operational and production environments.

Red Hat provides the platforms and tools to support the journey towards DevSecOps, as well as operational security including the development of security patches that are backported to older product releases.

Managing data at the edge means having to make decisions that protect sensitive information wherever it is processed. To address these security challenges,

organizations must set up controls and policies to maintain proper security postures, governance, and compliance. Security teams also need sufficient visibility to predict, detect, and address risks proactively so that intermittent connectivity does not disrupt ongoing operations, security, or compliance functions.

All these diverse operational challenges mean that intelligence and automation is needed in the application layer above the network to provide real-time protection and security. Security automation is critical to eliminating human error in configurations and monitoring that can cause security flaws and vulnerabilities. Using automated infrastructure, edge computing systems can be much more secure.

CUSTOMER SUCCESS STORY

In the process of evaluating Red Hat and its Edge offerings, we were able to hear from a customer on how Red Hat's platform has helped them achieve their goals.

Snam, one of the world's largest gas networks turned to Red Hat OpenShift to help drive company-wide digital transformation. With Red Hat's tools, Snam can better manage and scale applications across its infrastructure including at the edge. The organization was focused on developing a technology stack that could meet its IoT and data needs and connect up to 30,000 devices. From a security perspective, Snam used Red Hat solutions to manage clusters and applications at a number of edge locations. Red Hat solutions also helped the organization efficiently manage containerized content across data centers and to the edge, focusing on cloud-native and DevSecOps development models and environments.

How Red Hat is Addressing Edge Computing Security Worries

The growth and importance of edge computing is continuing to inspire a broad ecosystem of supported products and services to help make the technology more manageable for enterprises. Powering that growth is open source, which is becoming the prevalent approach to deliver on edge computing interoperability, security and ease of operation across public clouds, private data centers and edge locations. Industry veteran Red Hat is well-positioned for this market due to its ability to leverage a diverse ecosystem of providers and software vendors, its in-house innovation and its broad open source, device-agnostic platforms that focus on delivering security, automation and performance for organizational IT infrastructures.

Red Hat's broad product lines use a common platform and tool sets from edge to core to cloud, which help enterprises reduce the required skills needed to keep them running and deliver improved business value. Red Hat OpenShift, Red Hat Enterprise Linux (RHEL) and its other platforms provide operational consistency and portability of applications while ensuring consistent application lifecycles, hardened security and powerful development processes.

When building and operating mission-critical edge computing deployments, integrated and comprehensive security capabilities and protections are essential for success, making Red Hat an excellent partner candidate for edge environments. The need to drive robust operations is never more relevant when you factor in the sheer breadth and scale of edge computing deployments.

Red Hat has long led the market with its powerful open source platforms, expertise, services and commitment to its customers around the world. The edge computing marketplace is just the latest enterprise growth area where Red Hat's work, reputation and quality will help businesses take their technology infrastructures to the next level.