Automate data security

Multicloud financial services applications

The cost of data breaches will rise from $3 trillion annually to over $5 trillion in 2024, or an average annual growth of 11%.[1]

Juniper Research

Managing security and compliance across multiple clouds means mitigating multiple risks

In recent years, benefits like agility and elasticity have driven rapid adoption of cloud-native applications in the financial services industry. However, moving to cloud and multicloud deployments brings security and compliance issues to the forefront, especially when it comes to customer data. Protecting data represents a critical concern for every business, but in financial services it can mean protecting the customer's money as well.

Banks, payment providers, and insurers along with other financial service firms must comply with a range of increasingly strict security and privacy standards. These include the Payment Card Industry Data Security Standard (PCI DSS) and the European Union's General Data Protection Regulation (GDPR). Although a European law, many global companies are raising the bar to comply with GDPR, which requires stringent tracking, reporting, and documentation to maintain compliance.

Many of these laws contain specific requirements regarding how organizations protect personally identifiable information (PII) data. They also require companies to prove that they have safeguarded customers' data in the event data gets lost or stolen. For example, California's Security Breach Information Act (SB-1386) – which other U.S. states have also adopted – was the first state law to require breach disclosure. It mandates organizations notify affected individuals "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement."[2] However, it specifically offers a safe harbor if you can demonstrate that the compromised data was encrypted at the time of loss.

Failing to comply with data privacy regulations such as these can be expensive for financial services companies. Data breaches have soft and hard costs. A recent report from Juniper Research found that the cost of data breaches will rise from $3 trillion annually to over $5 trillion in 2024, or an average annual growth of 11%.[3] This increase will be driven primarily by increased fines for data breaches as regulations tighten.

Companies also risk substantial business losses as enterprises become more dependent on the digital realm. For instance, few in the financial services industry will forget the cost, brand damage, and business distraction suffered by Equifax when it failed to protect customers' PII.

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

1 *Juniper Research. The Future of Cybercrime & Security: Threat Analysis, Impact Assessment & Mitigation Strategies 2019-2024, August 2019.*

2 *California Senate Bill 1386, SEC. 2. Section 1798.29, enacted September, 2002.*

3 *Juniper Research. The Future of Cybercrime & Security: Threat Analysis, Impact Assessment & Mitigation Strategies 2019-2024, August 2019.*

Multicloud environments demand a compliance automation strategy

Hybrid and multicloud environments have rapidly become standard for financial services companies. According to a recent Enterprise Cloud Index report, financial services outpaced all other industries in the adoption of hybrid cloud, reaching 21% of the market compared to a global average of 18%.[5] In these mixed environments, manually monitoring system compliance becomes more difficult and, in many cases, nearly impossible.

A recent SANS Institute report found that more than half (54%) of organizations surveyed were adjusting their cloud strategies to meet evolving regulations.[6] Even so, financial institutions must migrate to the cloud to stay competitive.

54% of organizations surveyed were adjusting their cloud strategies to meet evolving regulations.[4]

SANS Institute

Without an effective automation strategy, IT teams face a number of potential pitfalls related to manually checking systems for security and compliance. Manual processes can lead to improper actions and configuration changes that lack audit trail information – a key component of compliance.

These manual processes are:

- Time-consuming and tedious.
- Prone to human error.
- Not repeatable, shareable, or verifiable.
- Vulnerable to audit failure as a result of incomplete and inconsistent changelog information.
- Inhibitive of communication between operations and security teams.

Fortunately, a sound automation strategy can help organizations improve their security and compliance, thereby reducing the overall risk to the business. Effective automation strategy can also help manage and streamline complex multicloud environments.

Automation allows financial institutions to manage security and compliance more comprehensively and efficiently. It also helps prevent human errors by automating software patches and system configuration. As Verizon stated in its 2019 Data Breach Investigations Report, "Cybercriminals prey upon human error."[7] This is another way automation aids compliance and overall security posture.

4 *SANS Institute. SANS 2019 Cloud Security Survey, 2019.*

5 *Nutanix. Enterprise Cloud Index, 2019.*

6 *SANS Institute. SANS 2019 Cloud Security Survey, 2019.*

7 *Verizon. 2019 Data Breach Investigations Report, 2019.*

Compliance as code: Automating cloud-based security

Automated strategies take DevSecOps to the next logical level: automating compliance as part of the process. Recently, it seems IT organizations are implementing all of their processes as code, and implementing compliance is no different. Similar to how pure DevOps evolved into DevSecOps—where several security validations are automated—we see the same starting to happen with compliance. Given substantial compliance requirements in financial services, it is no surprise that the industry would need to automate compliance as they coded security with DevSecOps. The result is DevSecComplianceOps.

Building compliance on a global scale is not easy, especially considering regulatory requirements are often locally specific. A global bank, for instance, will have to meet worldwide regulatory requirements along with regional regulations. For example, a bank in the European region could have additional compliance standards that are specific to its locations in Germany. Unlike a DevSecOps situation where code written for security works just as well in Malaysia as it does in Germany, many financial services organizations must meet both global and local compliance requirements.

Given its span across multiple geographies, that same bank may have different requirements to keep data behind the firewall. They may need to plan for future regulations that could require keeping data in more than one public cloud, ensuring business continuity and resilience. Changing regulatory requirements makes automating compliance even more important to manage complexity across multiple regions and cloud types.

Reducing risk and streamlining compliance effectively involves building compliance regulations into application code from the beginning. This new DevSecComplianceOps approach allows IT teams to achieve localized automation within a globalized framework, and to do it in a scalable, hardened environment.

Red Hat and Intel help automate security and compliance

Together, Red Hat and Intel provide the complementary hardware and software necessary for automation. These two innovators have also collaborated on joint solutions combining infrastructure-as-code technologies. In-depth partner initiatives have been in development for several years and the result is tightly integrated solutions with added benefits.

Red Hat® Ansible® Automation Platform automates infrastructure and code deployment—in any cloud environment—by using Red Hat OpenShift® container application platform technology. Combined with Intel Software Guard Extensions (Intel SGX)—which enables hardware-based isolation and memory encryption—data resides in trusted "enclaves" in memory. It can also be automatically and consistently deployed to local regions. Using this automated, consistent, and security-enhanced data environment as a foundation for digital business provides more code protection to help developers deliver more secure solutions.

Historically, regulated workloads had to run on a dedicated trusted environment, which usually meant dedicated infrastructure inside the bank. With technology that protects the data in use, workloads can share servers in one or multiple clouds. In other words, you can run your workload in a trusted manner even in an untrusted environment.

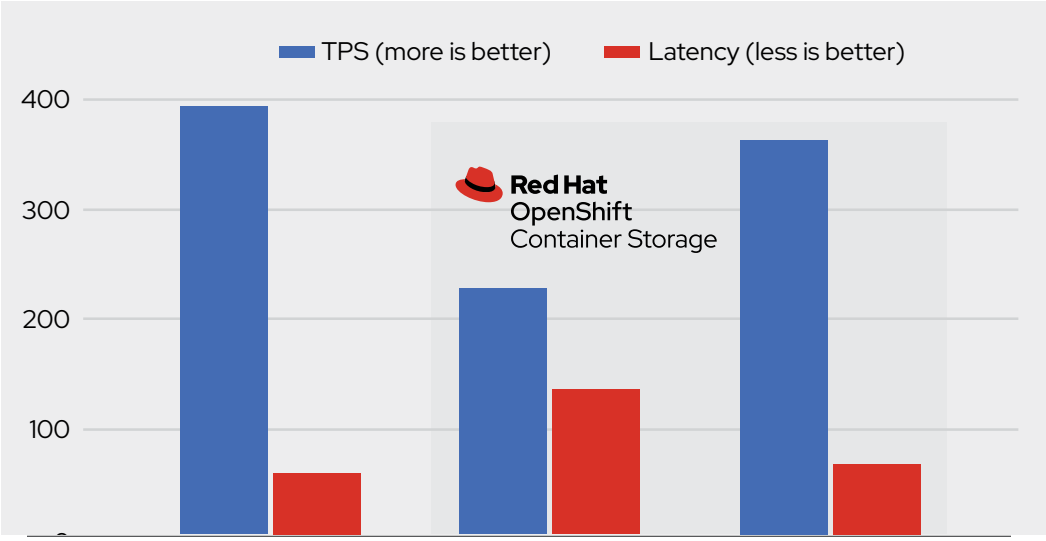

Figure 1. Intel SGX capable system

For instance, considering the stringent compliance requirements for GDPR, using different methods to protect data in Europe and the U.S. would be ineffective. Intel SGX allows developers to create a more secure enclave in memory, so even if attackers have physical access to a server or can maliciously elevate their administrative privileges, they cannot see what is running in memory.

Developers can create an automated system in code on Red Hat OpenShift with Red Hat Ansible Automation Platform. This approach provides evidence that an attack on a server restricted a bad actor from seeing what was executing in that enclave. Similarly, in any cloud where you must trust a third party, these enclaves can reinforce trust even when the environment is not completely trusted.

Before GDPR, it was possible for banks to go into the datacenter and discard a crashed physical disk. Post-GDPR, however, customers can demand that you delete their data and you must provide auditable evidence that the data was deleted or destroyed. One common practice is creating a compensatory mechanism that provides regulators with evidence that the data is no longer available because it was encrypted.

To illustrate, imagine a coffee company employee leaves a laptop with millions of customers' credit card information in a taxi. Under most privacy breach laws, the bank would be required to compensate the victims and provide public notification of the breach. But if the laptop had endpoint protection software that ensured its hard disk was encrypted, the need for compensation and notification is eliminated. As a compensatory mechanism, the software provides evidence of encryption.

In any cloud, compliance-as-code can provide a similar compensatory mechanism. In development, the cloud-native application that uses Intel SGX with Ansible Automation Platform provides a compliance automation wrapper around Red Hat OpenShift.

Conclusion

Red Hat and Intel can help your team bridge your continuous integration and deployment (CI/CD) pipeline and integrate compliance-as-code by design. Doing so can help reduce the risk of human error in the DevOps environment. This DevSecComplianceOps approach bridges gaps between development and operations teams by automating application building, testing, and deployment.

Automation consistency enabled by DevSecComplianceOps provides the ability to share and verify guiding repeatability, and provides a common automation platform across teams and clouds. Together, these capabilities give security, networking, Windows, Linux®, and other teams the information they need to do their part in enforcing security with compliance-as-code.

The compliance-as-code approach offers a number of benefits.

- Compliance traceability and repeatability
- Less time spent on repetitive tasks
- Reduced risk of downtime through a consistent infrastructure management approach
- Minimized risk of systematic errors through automated analysis, detection, and resolution
- Reduced risk of human error
- Accelerated IT processes (often from days to minutes)
- Consistent configuration and management across multicloud environments

Learn more

These examples provide a few simplified scenarios of how financial services firms can secure data and personal information in today's multicloud workloads using compliance as code. Learn more about how Red Hat and Intel unlock the CI/CD pipeline automation – without compromising security or compliance.

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
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
#F24716_0820