Security and Compliance Automation for Financial Services

A GUIDE TO CHOOSING SOLUTIONS

AS ORGANIZATIONS INCREASINGLY TURN TO HYBRID PUBLIC AND PRIVATE CLOUDS to ensure uptime, accelerate innovation, and meet customer service demands, they confront a unique set of security challenges.

A 2019 report by the SANS Institute found that 19% of organizations surveyed had experienced unauthorized access to their cloud environments, up from 12% two years before. Survey respondents cited unauthorized access as their No. 1 concern around cloud environments. More than half of the respondents also expressed concern that they couldn't tell what data of theirs was being processed in the cloud.

Recent high-profile cloud-based attacks, such as the ATP 10 attacks that surfaced in late 2018, further add to the concerns of organizations depending on cloud environments. Increasingly stringent regulatory standards also challenge organizations charged with safeguarding and monitoring critical data. The SANS Institute report found that more than half (54%) of the organizations surveyed were adjusting their cloud strategies to meet evolving regulations.

All of these challenges hit the financial services industry particularly hard. For them, data quite literally is money, and companies are especially vulnerable to reputational damage. Even so, institutions must migrate to the cloud to stay competitive.

"Hybrid environments are becoming the norm in financial services companies," says Lucy Kerner, senior principal security global technical evangelist and strategist at Red Hat. "In this mixed environment, manually monitoring systems for security and compliance becomes more difficult and, in many cases, impossible."

Fortunately, an automation strategy can help improve the security and compliance of an organization and reduce the overall risk to the business. This guide will help you assess your needs in the area of security and compliance automation and enable you to make informed choices.

AUTOMATION FOR IMPROVED SECURITY AND COMPLIANCE

Automation doesn't just help institutions manage security and compliance more comprehensively and efficiently. It also helps them avoid human errors by automating the configuration of systems and software patches. That further aids security because, as Verizon's 2019 Data Breach Investigations Report affirms, "Cybercriminals prey upon human error."

Another benefit that automation provides is visibility and control of the entire mixed environment, getting everyone in the enterprise on the same page regarding security and compliance.

That visibility and control extend not just to data, but also to information about system configurations and software updates and security patches, which is crucial. Visibility and control can also take in automation workflows across all systems. That's important too, because as Kerner says, "Automation helps with controlling who gets to launch what automation task when."

Despite all the benefits, the challenge of choosing the right solutions can delay deployment. Use this checklist to help you assess the capabilities you need in security and compliance automation.

ASSESSING YOUR CAPABILITIES

Evaluate your automation needs based on the following areas:

Centralized Visibility and Control. Today's complex, mixed-hybrid-cloud infrastructures present significant challenges to getting a big-picture, centralized view of the security and compliance status of enterprise systems. In addition, many legacy security tools do not work in the cloud or in hybrid cloud environments.

54%

of the organizations surveyed were adjusting their cloud strategies to meet evolving regulations. SOURCE: SANS INSTITUTE REPORT

Ensure the systems and tooling that you evaluate provide centralized visibility and control, along with centralized automation capabilities for all of your critical systems—whether they're on-premise or in private and public clouds.

Security. As a financial institution, you want to minimize security risks to your business. Choose security automation accordingly.

Red Hat® Satellite, for example, automatically monitors systems and provides the ability to apply security patches at scale as soon as they are available. Any solution you choose should be able to perform both functions—security scanning for both vulnerabilities and configuration compliance, and automated patching—without manual effort.

Automation should also enable administrators to reliably and repeatably provision secure systems. "This capability allows you to eliminate snowflake systems and ensure that no untrusted changes take place without anyone noticing," says Kerner.

Compliance. Besides scanning for security vulnerabilities, automation should also scan for compliance issues across hybrid cloud environments, including checking for compliance with a range of standards relevant to the financial services industry.

Red Hat's OpenSCAP National Institute of Standards and Technology (NIST) scanner provides the ability to scan and remediate vulnerabilities and security compliance baselines. This tool is built into both Red Hat Enterprise Linux® and Red Hat Satellite and ensures that systems under its purview meet the following standards and more:

- Payment Card Industry Data Security Standard (PCI DSS)
- Security Technical Implementation Guide (STIG)
- National Institute of Standards and Technology (NIST) 800-171
- Operating System Protection Profile (OSPP)
- Red Hat Corporate Profile for Certified Cloud Providers

Reporting. Advanced solutions allow for robust and feature-rich reporting on systems to aid in compliance audits and enhance security. Reports should be centralized and provide easy access to anyone who needs them. That includes team members whose job it is to provide evidence of compliance to internal or external auditors.

"Many security standards have hundreds of security controls," observes Kerner. "You want to make it as easy as possible to prove to the auditor that you are passing the requirements of any relevant standard or custom security policies that are specific to the organization."

Red Hat's vulnerability and compliance scanner, OpenSCAP, for example, lists the state of compliance for all the security controls for a given standard with simple color-coding. The coding shows passed or failed security controls at a glance. A security control marked in red indicates that a given system doesn't meet that standard, while green indicates that the system does meet that particular checked security control. OpenSCAP also includes tools to remediate the failed security controls.

Compliance reports should list which controls are not being tested, along with explanations for why not. In addition, compliance reports should clearly indicate how to fix the failed security controls and ideally provide native tooling to automatically remediate the failed security controls for any given security standard.

Centralized Automation. This capability is vital for extending the benefits of security and compliance automation across hybrid cloud environments, as well as for ensuring consistency across systems and teams within an organization.

Here's what to look for in automated solutions:

- Visibility into all automation workflows, including information about who is running what automation and when
- A central repository for automation scripts
- Centralized role-based access control for all automation to control who can run the various automation scripts
- Centralized automation logs documenting which automation scripts have run where, by which person(s), and on which systems

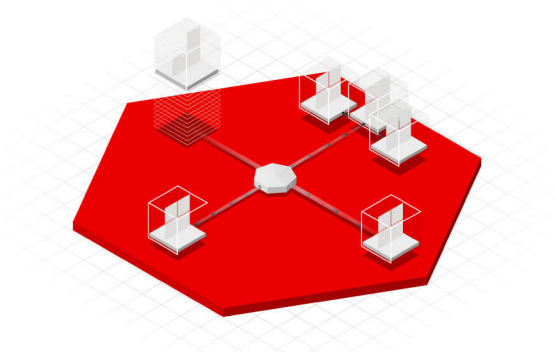
SECURITY AND COMPLIANCE BAKED IN

No set of tools, however capable, will solve all of an organization's security and compliance needs. That's because, as Kerner puts it, security isn't a product. Instead, it's a continual process that requires the participation of everyone in the organization.

A consistent automation strategy, using an automation language that all the disparate teams in the organization speak, is key to powering this participation. This automation consistency provides the ability to repeat, share, and verify. Together, these capabilities give not only security teams, but also networking, Windows, Linux, and other teams, the information they need to do their part in ensuring security and compliance. In the realm of configurations, for example, "Whether it's how applications or systems are configured, the knowledge shouldn't stay stuck in anybody's head," says Kerner. "All of that knowledge should be transferred to an Ansible Playbook or to automation scripts. This knowledge transfer from a single person to code enables both security and compliance-as-code, which guides that repeatability and ability to share—all critical ingredients to avoid long-term problems."

Although there's no silver bullet for security and compliance, you need to ensure that the security solutions you evaluate include security features "baked" in—that is, features included in the initial design phase.

"Security should not be an afterthought," says Kerner about deploying new applications. "Security should be continuously integrated throughout the application and infrastructure, not just by using third-party security products, but also by taking advantage of the built-in security capabilities of technologies you already have, such as your OS, application platform, automation tools, and more."



SOLUTIONS FROM RED HAT

Red Hat helps organizations build security in from the start with consulting services, residencies, and courses. Red Hat also helps build security into applications with its open source middleware offerings and Red Hat OpenShift® Container Platform for both legacy and containerized applications.

Red Hat also provides a more secure platform, starting with Red Hat Enterprise Linux and extending through all of the solutions that run on top of it.

Finally, Red Hat provides the automation and management tooling to help continuously monitor, manage, and automate systems for security and compliance and help organizations continuously adapt as the security landscape changes.

For these reasons and more, financial institutions increasingly turn to solutions from Red Hat for automated security and compliance.

For example, a bank serving 16 million customers needed to update its inconsistent process for patching the software running its systems. Business managers and security teams knew that missed patches exposed the bank to the risk of hacks, along with accompanying dips in customer confidence, potential fines, and legal action.

The bank turned to Red Hat to design automated workflows for patch management. IT managers then deployed the new workflows throughout the bank's infrastructure. Today, all systems within the bank's IT environment automatically and consistently get patched on a defined schedule, fixing security holes even as they emerge.

As the financial services industry looks to hybrid infrastructures to meet the demands of the always-on economy, security and compliance become ever-more significant challenges. As Red Hat's banking customer demonstrates, automation can make all the difference in meeting those challenges.

NEXT STEPS

Security and compliance automation not only helps reduce the security risks associated with human errors, it can also relieve the pressure on beleaguered IT departments, freeing them up to focus on business operations and innovation. Automation and management solutions from Red Hat can help enterprises meet the hybrid cloud challenge by providing visibility, control, and security across a hybrid environment while aiding compliance, all with the help of automation.

"Automation improves security, risk, and compliance," says Kerner. "It allows you to proactively monitor and remediate continuously throughout both the infrastructure and application life cycle." And that makes it a vital component of any security and compliance effort.

Learn more about Security Automation for Financial Institutions **here**.