Maintaining SECURITY & COMPLIANCE is EXHAUSTING

OpsMx can help Simplify

Maintaining Security and Compliance is Exhausting

Security

Developers at all leading companies must create software while maintaining security and complying with policies. These initiatives may appear to be at odds with the concepts of rapid delivery, since compliance efforts concentrate on improving safety and continuous delivery concentrates on increasing speed.

Security and Compliance Are Maximum Priority Requirements

OpsMx customers report that they have successfully enhanced both speed and security by addressing the following challenges directly.

Problem

08 Inconsistent policy management

09 Increased security vulnerabilities

10 Insecure software delivery

11 Poor traceability and observability

08 Inconsistent policy management

Compliance with internal and regulatory policies (for example, SOX) is a non-negotiable requirement in software delivery, but it is frequently difficult to assure. Reasons include:

- The number and complexity of policies seem to continually increase.
- Changes to policies are frequent, so keeping current is a continual challenge.
- Policies differ between different geographies and different applications.
- Enforcement and validation of the policies across all teams and all updates is usually manual and therefore slow and prone to error.

09 Increased security vulnerabilities

Preventing security breaches in software delivery has similar challenges to policy compliance, with one addition. Security compliance is complicated by the presence of the security team. Although development, delivery, and security teams share common goals, overlapping responsibilities and skill sets sometimes slow deployment.

09 Insecure software delivery

Recent news - the security breach at hundreds of organizations through the vulnerability introduced through SolarWinds[1] - has highlighted the importance of ensuring that the delivery process itself is secure.

Organizations must secure the entire software delivery system and processes, with tools and best practices, across three dimensions: securing access to the system, securing the system itself so that no malicious software can be introduced, and ensuring that all teams follow security protocols.

10 Poor traceability and observability

There are two main issues in policy and compliance that can be solved with improved visibility.

Observability and traceability

The first issue is overall traceability and observability. This is needed to ascertain the who, what, when, and where of any specific update or any group of updates. This information can increase security by locating all services that are dependent on a given artifact, help identify the probable root cause of errors, and identify trends that need to be addressed.

Reducing the time and effort of audits

The second issue is reducing the time and effort of audits. Maintaining policy compliance is difficult enough. Organizations must also be able to prove that they are compliant. Reducing the cost and time of required audits is key to successful software delivery governance.

Multiple companies have chosen to work with OpsMx specifically for our expertise in security and compliance.

[1] See this article for detail on the SolarWinds breach.
https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-1

OpsMx Customers Are Secure and Compliant

Leading Financial SaaS Provider

This customer provides the leading collaboration platform for financial service companies. Security in the financial industry is a basic requirement - without a completely trusted system, use of the solution would cease.

The Challenge

Enhance security of Continuous Delivery

Security is etched into the DNA of our customer that provides a collaboration platform for the financial industry. They needed to be certain that their new CD solution would strengthen - not weaken - security and policy compliance.

Security and policy compliance

- Because every single developer uses the new CD solution based on OpsMx Enterprise for Spinnaker (OES), automation of their deployment processes ensures that regulatory rules, internal policies, and security protocols are followed, or the pipeline is halted for review.
- This reduces the work for developers, SREs, and security teams. For example, a security approval for each production update is required, and it is verified simply using OES.

Securing the CD system

OpsMx specializes in creating a secure CD solution. Some of the special features of OES that this company implemented include:

- Integrations with their LDAP and MFA systems so that only authorized users are allowed to promote changes or to modify pipelines.
- Secure communication between all software components to defend against attacks by malicious actors.
- Automated security best practices throughout the development and SRE teams.

Audit and visibility

As part of the regulatory process, our customer is audited regularly. OES speeds the audit process and reduces the impact on developer productivity. Additionally, compliance with internal policies and security protocols are easily proven to internal and external stakeholders.

The Result

- Enhanced visibility and Security
- Faster and easier audit

The resulting secure CD solution provides confidence to the entire organization that updates are not only fast, but also secure and compliant. Further, it enables the company to use enhanced security as a competitive differentiator.

OpsMx Customers Are Secure and Compliant

A 150-Year-Old Banking Institution

The customer is a multinational banking and financial services company that serves their customers online and in person across 22 countries. Like all financial institutions, security and compliance are table stakes.

The Challenge

Implement a new CD process for software delivery and maintain market-leading security

One of our banking customers, with operations in some of the world 's most dynamic markets, was concentrating on improving the customer experience in their retail banking division. They adopted OpsMx for Spinnaker (OES) to enable continuous delivery.

Of course, the bank needed to maintain the highest standards in security throughout the delivery process. As part of their security protocol, their important customer-facing applications run in an air gapped environment.

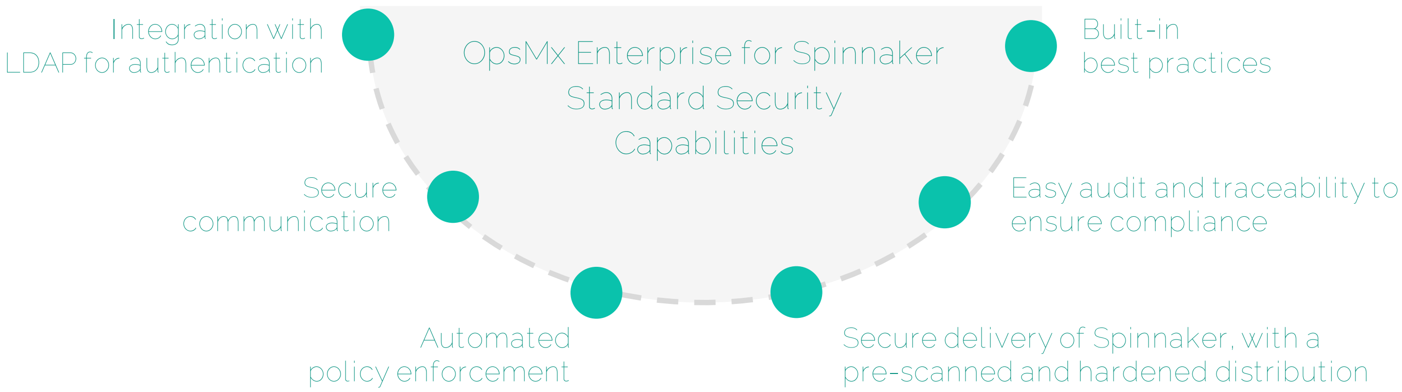
Open-source Spinnaker does not support air gapped environments.

OpsMx Enterprise for Spinnaker does.

The Result

With OES implemented, the customer unlocked many security benefits

In addition to addressing the air gap requirement, the company implemented an automated verification process using OpsMx Enterprise for Spinnaker. This automatically evaluates the risks of any update before deployment to production. If the risk is too high, OpsMx Enterprise for Spinnaker will fail the pipeline and send the update back to the team for further evaluation.



OpsMx Enterprise for Spinnaker Standard Security Capabilities

- Integration with LDAP for authentication
- Built-in best practices
- Secure communication
- Easy audit and traceability to ensure compliance
- Automated policy enforcement
- Secure delivery of Spinnaker, with a pre-scanned and hardened distribution

OpsMx Customers Are Secure and Compliant

A Leading Telecommunication Provider

This telecommunication company serves consumers and businesses. Security of communications is an absolute requirement for their customers, and that permeates their development and SRE teams.

The Challenge

Ensure highest security for a team with few resources

Software security has always been a top concern for this telecommunications firm. Strong security is one of the reasons they chose Red Hat OpenShift as their container platform for new applications. They also chose to implement a new continuous delivery solution to deliver updates more quickly.

The Result

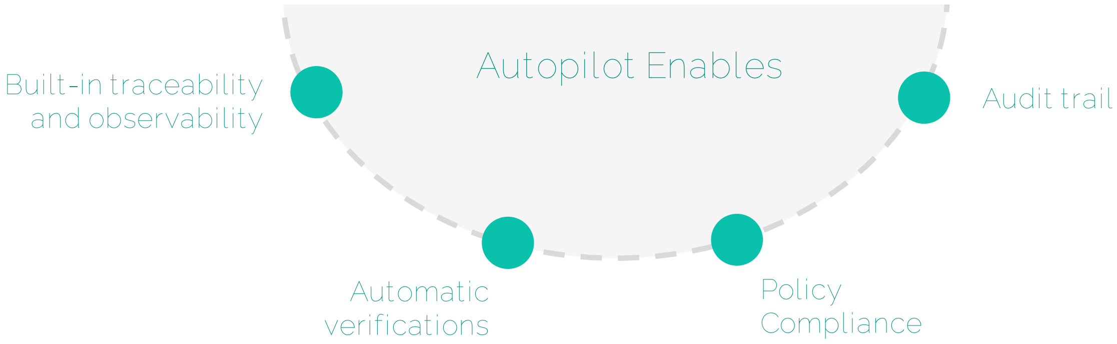
Simple security and policy compliance, automatically

They chose OpsMx for simplicity, speed, and security. During the implementation, they quickly added proper authorization and authentication protocols leveraging their existing LDAP system to ensure correct access.

OpsMx Enterprise for Spinnaker (OES) also provided built-in traceability and observability, reducing the effort and time required to track down details about specific updates.

Finally, the team deployed Autopilot, the ML-based module of OES. Autopilot automatically verifies that new releases pass quality, performance, and policy checks. If any policy or security vulnerability is found, the system notifies the SRE team so they can evaluate whether the update should be promoted.

Working with OpsMx, the team is confident in the quality of their updates and the security of the overall CD solution. Overall release quality has skyrocketed: they now claim that zero problems due to the delivery process reach production, and they have solid documentation of their policy compliance.

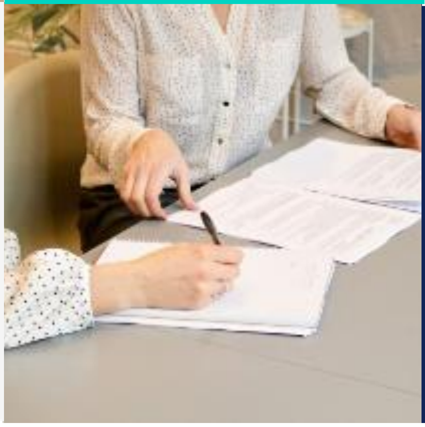


SECURITY

OpsMx

www.opsmx.com

info@opsmx.com



https://www.opsmx.com/contact.html