Navigating your journey to the Cloud...

CloudOrigin

The Cloud is not a static environment. Cloud Service Providers (CSPs) are adding new features on average every 4.16 hours. It is not that the Cloud is unstable, it is just that it is highly dynamic. And the controls you set to govern how Cloud Services are deployed to support your business applications need to reflect these changes as well as reflect the evolution of the Cybersecurity threat landscape.

CloudOrigin® represents the underlying Cloud Services controls repository and Cloud knowledgebase that underpins the CloudAtlas® suite. CloudOrigin® is designed to be your authoritative source of revision control on how your organization uses its Cloud Services resources.

CloudOrigin® helps to manage the dynamic challenges that enterprises using Cloud Services face in running their most critical business applications by creating an unambiguous set of answers to the following:

- What are the enterprise standards for PaaS and application-level settings based on Cloud IT controls policies and best practices?
- How do we know if line of business applications, once re-factored, or built from the ground up, will be in compliance once deployed?
- As Cloud environments are evolved by CSPs, applications are enhanced by developers, and/or controls are updated due to emerging threats, how will compliance "drift" be monitored, reported and remediated quickly?

Key Benefits

Risk Management oversight capabilities for Cloud-based applications.

Applications that are developed and monitored against consistent standards and controls.

Security controls that are closely managed and quickly updated to keep pace with Cloud evolution.

Lowered costs of Cloud operations, application compliance monitoring, and ongoing remediation.

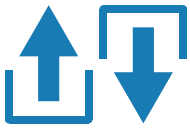
Key Capabilities

Having IT controls baselines for Cloud Services for high priority or regulated applications is an important risk mitigation approach. CIOs, CISOs, and IT Risk Management professionals can define their standards for Cloud-based applications through policies and Cloud service security-related settings.

Developers are not often not Cybersecurity or IT Controls experts. Layered on that, they may be new to the realities of developing applications for the Cloud. Developers can quickly focus on the baseline controls and settings they need to use as they deploy and manage their applications in a Cloud environment.

In the management of Cloud Services and the applications that run on them, there are many roles that are involved. Developers, risk management teams, and Cloud subscription owners. Given the importance of CloudOrigin® as both a developer and risk management tool, role-based access control is assigned to appropriate personnel only.

Cloud Services managed by a CSP still need to meet your IT control requirements. Understanding who, how and when changes have happened regarding specific Cloud Services instances deployed is part of good IT control requirements. The ability to track via audit trail who made what changes to the knowledge base is critical.



Given the frequency with which CSPs upgrade their platforms, the options for control settings increase as well. Staying with these changes at "Cloud Speed" requires fast updates. CloudOrigin® can import settings from a Cloud provider and easily integrate that into the development environment.

Enterprises successful in using and controlling Cloud Services know that no one individual can possess all the required knowledge. CIOs, CISOs, and IT Risk Management professionals responsible for defining and maintaining Cloud service settings can easily update CloudOrigin® to reflect the latest regulatory requirements.

Contact

Phone: +1-800-535-7443
Email: info@unifycloud.com
Web: www.unifycloud.com
Solutions: www.cloudatlasinc.com

UnifyCloud

Inc. 5000 #353 2015

Microsoft Gold Partner