UNISYS | Securing Your Tomorrow®

# CLOUD SECURITY AND COMPLIANCE

## Leverage Automated, Continuous Cloud Security and Compliance

### HIGHLIGHTS

- *Multi-cloud security and compliance through a single unified console*
- *Automated regulatory and security updates*
- *Real-time remediation and reporting*

## Industry Challenge

### Need for Security and Regulatory and Security Compliance

Current methods, tools and services for ensuring security and regulatory compliance of cloud infrastructures are inadequate, leaving most cloud users with few solutions to address their evolving needs. Shortcomings include:

- Inability to discover, assess, and manage cloud security and compliance posture on a continuous, comprehensive, system-wide basis
- Difficulty to keep up with regulatory and security guidelines that rapidly change
- Difficulty delineating and addressing shared security responsibilities of cloud and multi-cloud security across multiple vendors
- Lack of a comprehensive Cloud Security Posture Management (CSPM) system with cloud workload protections (CWPP)

Clearly, a system wide CSPM strategy to simplify security and compliance is needed. In fact, Gartner estimates that through 2024, organizations implementing CSPM will reduce cloud-related security incidents due to misconfiguration by 80%.[1]

[1.] Gartner. “Innovation Insight for CSPM.” January 2019.

# Continuous Cloud Security Posture Management

CloudForte® Assure™ provides continuous, real-time security posture management and regulatory compliance best practices for your cloud and multi-cloud environments. CloudForte Assure service includes:

- Assessment and management of multi-cloud security and compliance posture through a unified console and reporting
- Automated security and compliance configuration updates, such as PCI, HIPAA, GDPR and thousands of other polices and guidelines
- Implementation of real-time, continuous security and compliance policies to ensure that all your cloud infrastructure resources are securely and compliantly configured, including IaaS, PaaS and SaaS
- Compliance and security policies implemented to ensure that your critical OS/VM/Kubernetes/containers/O365 subscribers are secured and safe

## 24X7 Discovery, Reporting and Remediation

CloudForte Assure continually assesses, prioritizes, remediates, and monitors your cloud and multi-cloud infrastructures for real-time security posture management. This continuous cycle of preparedness is driven by best practice security and compliance policies, which can be augmented and expanded at any time. Currently, CloudForte Assure supports over 1,900 AWS and Azure cloud best practice security and compliance framework recommendations, including the latest NIST, CIS, and CSA cybersecurity standards.

CloudForte Assure is not only able to continuously scan for thousands of potential vulnerabilities in your environment, but also prioritize and fix or recommend remediation options for you in real-time. Its multi-vendor, multi-cloud architecture seamlessly assesses your mixed cloud environments from a central console and generates on-demand reports for analysis and use in periodic governance audits.

## Holistic Hybrid and Multi-Cloud Security

All Unisys Cloud Services operations are deployed using a security first approach that makes certain all infrastructure and processes meet or exceed industry best practices. Unisys Cloud services can optionally incorporate Unisys Stealth®, the only security solution that gives you the ability to see, segment, and secure the entirety of your global infrastructure. Out of the box. In less than an hour. Using a single, holistic security policy powered by irrefutable identity-based-access management. Its technology is so secure, Stealth™ is used in many high-security government and military applications.

## Personal Information Liability and Custom Assessments

With the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) becoming law, inadvertently exposed personal information can become a serious, finable liability for organizations.

CloudForte Assure discovers and flags the presence and potential vulnerability of Personally Identifiable Information (PII) and Personal Health Information (PHI) in databases and storage accounts throughout multi-cloud environments.

## Cloud Native Security

With the rising adoption of cloud native applications and microservices Kubernetes has become more vulnerable to cyberattacks and compliance scrutiny. CloudForte Assure now applies its comprehensive security and compliance protection to cloud native environments. Benefits include:

- Identify Kubernetes security misconfigurations
- Discover and assess Kubernetes containers and cluster-level hardening configurations and compare them against defined security policies
- Discover and remediate Kubernetes vulnerabilities before there is a breach

## Unisys Cloud Services Security-First Best Practices

CloudForte Assure is a key component of the Unisys Cloud Services commitment to architecting and serving best practice, security-first cloud and multi-cloud environments. The full range of Unisys Cloud services range from initial consultation, through full cloud implementation, to system management, and ongoing support.

**For more information, see www.unisys.com/Cloud.**