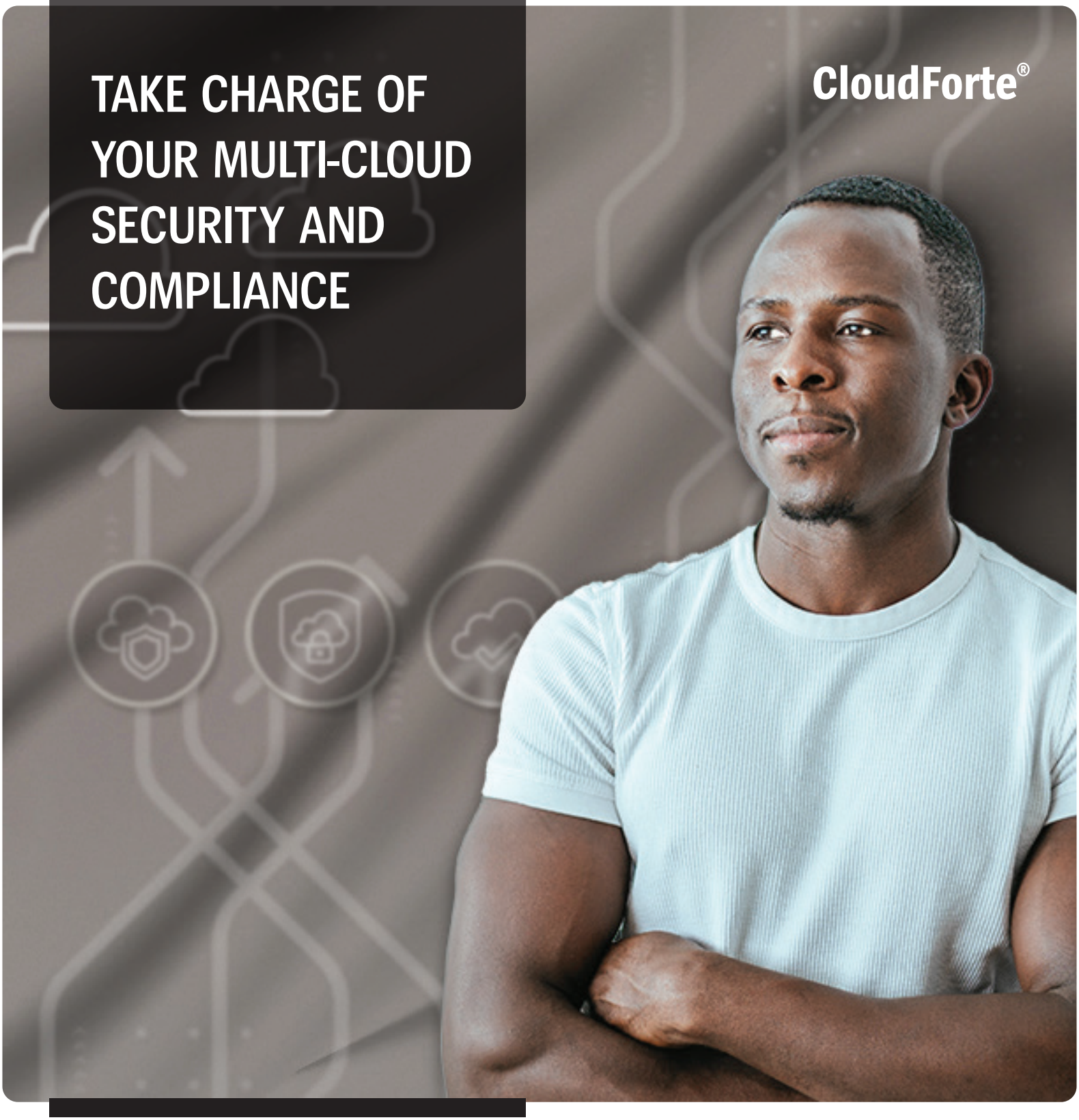
TAKE CHARGE OF YOUR MULTI-CLOUD SECURITY AND COMPLIANCE

CloudForte®



CLOUDFORTE® ASSURE™

UNISYS | Securing Your Tomorrow®

Multi-Cloud Is Secure — but Most Deployments Are Not

We hear a lot about cloud security lapses and high-profile breaches in the news. Industry reports and analysts exhaustively cover sensational cases publicly. But if you dig deeper into the details of these breaches, you'd discover that many of these vulnerabilities could have been avoided if the cloud environment was configured according to cloud security and compliance best practices. Cloud is secure. However, most cloud deployments do not comply with security guidelines. Here is an uncomfortable cloud security projection:

> *"Through 2025, 99% of cloud security failures will be the customer's fault."*
>
> *– Gartner.*[i]

Analysis finds that most cloud customers are not intentionally lax in their approach to security and compliance, but instead, do not have the tools, knowledge, and processes to implement cloud security and compliance effectively. In the on-premises world, systems do not change as frequently, and the manual process of security assessments work. In the cloud, with the dynamic nature of these environments, it is impossible to control security manually. But cloud needs continuous re-examination and remediation, especially in fast-paced DevOps environments.

Cloud adopters may not be fully cognizant of all current and evolving cloud security best practices. Two main factors that hamper best practice cloud security adoption are a lack of cloud platform-specific knowledge among staff involved in cloud configurations and the lack of automation for infrastructure deployments. Cloud security is different from on premises security models, therefore cloud-appropriate security and compliance must be established prior to cloud migration.

Security is also closely entwined with how cloud infrastructure is used. Every component of cloud has distinct security requirements — compute, VM, storage, network, containers. And each infrastructure component has its own unique security requirements.

Moreover, how applications and services utilize these resources and what cloud-specific security mechanisms are used is also differ with each cloud vendor. Therefore, in-depth pre-planning for security is a must, and continuous security and compliance checks thereafter should be mandatory. However, it is understandable that many professionals simply "don't know what they don't know."

Cloud Blind Spots

In a recent roundtable, top enterprise security professionals felt one of the greatest challenges in securing cloud was the lack of visibility into their company's cloud deployments. It is no wonder. Well over one thousand compliance best practices exist, and each must be handled differently depending on the platform (IaaS/PaaS) or vendor (AWS/MS Azure/Google, etc.). In addition, frequent upgrades in components such as storage, network topology, and workloads must be rechecked after each change. Point-in-time security assessments don't show the real picture anymore.

> *"A vast majority (67%) of survey respondents say it is more difficult to protect sensitive data in cloud computing environments using conventional security."*
>
> *– Global Cloud Security Survey.*[ii]

Using on-premises security practices in the cloud may only go so far. As clouds grow — in size and number — on-premises security measures cannot fully and compliantly prepare workloads and data in the cloud. Security teams struggle to track, analyze, and document this security — often using rudimentary spreadsheets and home-grown project dashboards.

Too Many Moving Targets

Further complicating security and compliance is the ever-evolving nature of threats and the necessary evolution of security best practices. Security and compliance guidelines can change frequently to accommodate threat environments, system vulnerability discoveries, and new regulatory requirements, such as data privacy. For example, the European Union implementation of the General Data Protection Regulation (GDPR) cost companies worldwide hundreds of millions of dollars and countless preparation hours to meet its requirements. With fines up to $1200 per employee, even the smallest organization had significant incentive to comply. There are similar regulations on the horizon in United States with the California Consumer Privacy Act, which will require a whole new round of compliance checks and security audits.

> *"Seven in ten organizations have put systems into place that will not scale as new regulations emerge."*
>
> *– CPO Magazine.*[iii]

Meanwhile, NIST, PCI, HIPAA, and dozens of other security benchmarks and regulatory compliance requirements demand increasing levels of system and security expertise. Complexity is further multiplied when moved from on-premises to the cloud — especially multi-cloud.

Shared Responsibility, Multi-Cloud Use — and Risk

Cloud security is a shared responsibility. All major vendors provide details of what security they provide, and which elements the customer must address. The ease of deployment to public clouds can make security compliance especially prone to failure. Many deployment processes are performed without complete IT security oversight. This lack of holistic planning is a recipe for misconfiguration. Also, due to the growing use of multi-cloud environments, applications, processes, and data traverse multiple cloud platforms with differing architectures — none of which map directly to on-premises models. Complexity is further complicated with DevOps, where apps and services rapidly evolve and change over truly short timelines. Even when things are automated, it doesn't mean deployment automation necessarily configures the environment securely.

DevSecOps: A New Security Center

While regulatory bodies put stringent requirements on compliance, market competition and innovation are even greater stressors on system security. In response to the push for rapid innovation, agile DevOps teams can run literally hundreds of iterations of their code in a short period of time. Traditional, on-premises security procedures, if implemented in such an environment, would slow down delivery cycles and needlessly complicate this iterative development. Therefore, with so many changes rolling out over such short development cycles, it has made most sense to move security of these applications closer to their inception or left shift: DevSecOps. Security validation in cloud app development then becomes 'baked into' the application development lifecycle.

For this model to be truly effective, however, tools and processes for security and compliance must work in tandem with the DevOps processes and CI/CD pipelines.

> *"We look at security and compliance investments as an enabler of trust ...when people have that trust, they're better able to leverage the benefits of moving their applications and workloads to the cloud."*
>
> *– Tom Patterson, Chief Trust Officer, Unisys.*[iv]

A Recipe for Success: Security and Compliance Throughout Cloud Lifecycle

A solution for insuring security and compliance amid the rapid changes within cloud is to adopt a continuous security assurance — Cloud Security Posture Management (CSPM). A CSPM product pulls out actual cloud workload configurations, compares them against defined security policies, and identifies deviations from the standard. The software enforces security posture by logging tickets and sending notifications when it identifies misconfigurations, providing remediation guidance for manual corrections and executing auto-remediations whenever possible.

By using CSPM concepts and tools, enterprises can:

- Achieve greater visibility into a security posture across all cloud environments, including multi-cloud
- Assess configuration of cloud resources for adherence to cloud security best practices
- Check all new or modified services prior to release into production
- Integrate security management into existing application development lifecycles
- Incorporate continuous compliance system-wide
- Deliver consistent risk management and analysis across apps, services, workloads, and vendors

A strong and comprehensive CSPM program encompasses both operations and development, each providing data for the assessment of risk and the ongoing adjustment of policies and controls to maintain compliance (See Figure 1. Source: Gartner).

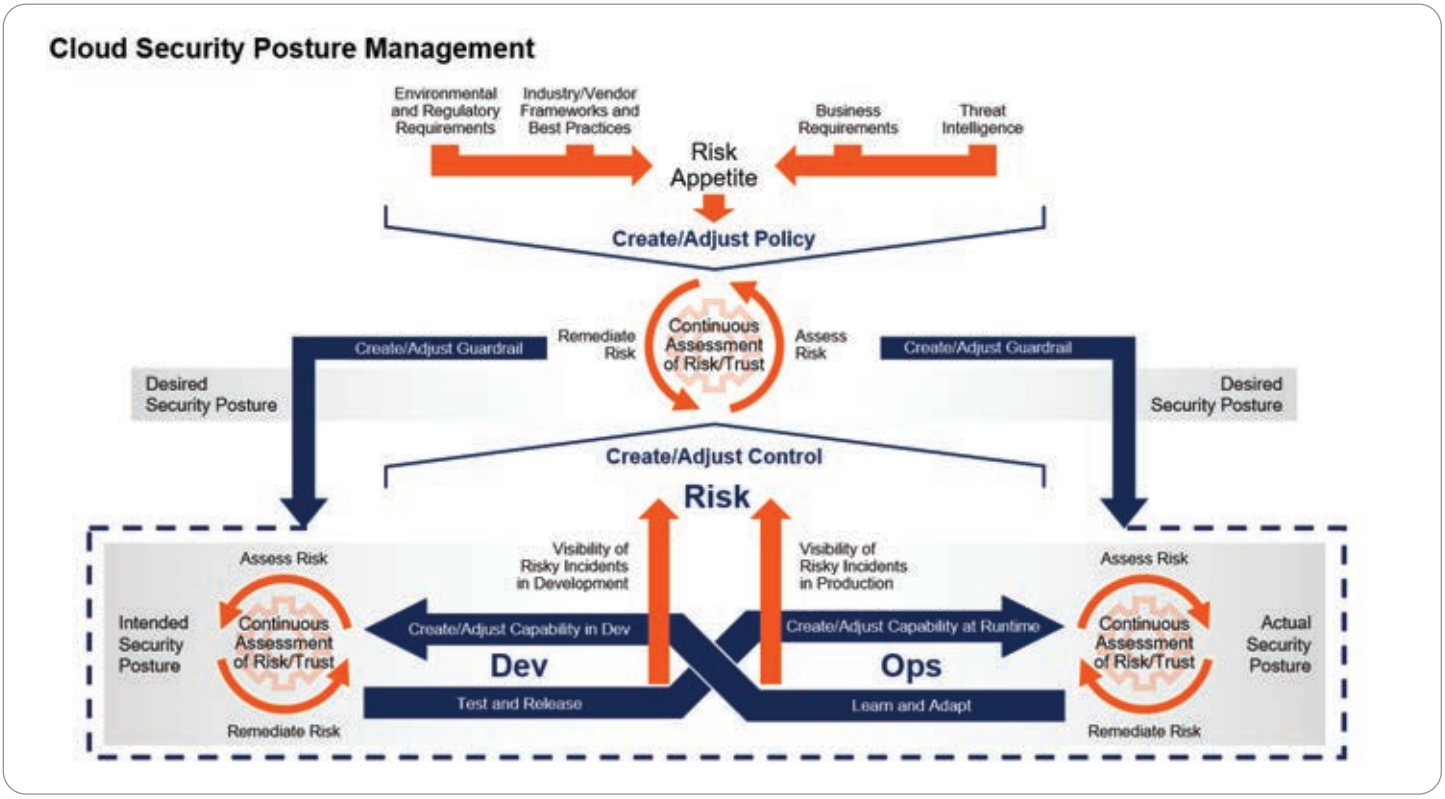


Figure 1. Cloud Security Posture Management. Source: Gartner 2019.

Application of this process through best practices management, assessment, and tools will greatly reduce the chance of non-compliance.

Gartner estimates that through 2024, organizations implementing a CSPM offering and extending it into development will reduce cloud-related security incidents due to misconfiguration by 80%.[v]

Cloud Security Posture Management Goals

No security management system can fully guarantee 100% cloud security compliance, however, using CSPM can dramatically reduce the risks associated with cloud misconfiguration, ensure better adherence to cloud security best practices, and alert security professionals of potential vulnerabilities. An effective and efficient CSPM offering will deliver the following:

Application of constantly evolving industry and security compliance standards. Tools and processes must be in place to compare cloud security best practices and guidelines to the customer's cloud environment configurations, regardless of cloud provider. Common standards include NIST, CIS, PCI-DSS, HIPAA, and many others that are industry specific.

Exhaustive and up to date compliance best practices knowledgebase. As policies and standards change, so too must CSPM. In addition, no two businesses are alike, and any useful CSPM must make allowances and embrace internally developed and adopted security policies wherever needed. As industry standards and best practices change, the CSPM process must make timely updates to its knowledgebase to provide the best possible outcomes.

Mapping of compliance for the cloud. During migrations or in the construction of new deployments, customers need tools to define their minimum set of "must have" security policies for their cloud – a security baseline.

Continuous assessment and remediation. Even day-to-day assessment may not be enough to ensure adequate security and compliance. As changes occur in the cloud, they should trigger automated scanning, assessment, and where needed, remediation. All of this should happen prior to release into DevOps production environment. CSPM is most effective when implemented throughout the application development life-cycle—from its design to its deployment and ongoing operations.

CSPM can play a pivotal role in all phases of cloud adoption:

New Cloud

In new cloud designs, architects must think of preventative security measures first, using industry standard compliance guidelines for the complete reference architecture across both application and cloud infrastructure. Incorporating security in the earlier stages of development lifecycle leads to much better security posture of the production environment. When preventative measures are not fully implemented, the results can be security breaches. Even higher investments in detect and protect methods such as threat detection, forensics, and others may not help.

Migrations

During cloud migrations, it is important to identify what security policies are essential to properly configure the cloud infrastructure before deployment of a legacy system into production, especially in multi-cloud environments from multiple vendors.

Operations

Once live in the fully working environment, systems should undergo continuous security, compliance, risk, and data privacy monitoring. Automated alerts should detail any non-compliance instances in real time, allowing for remediation on the spot. In addition, the CSPM knowledgebase should be updated with the latest cloud security best practices, incorporating the latest in cloud security and compliance regulations.

CloudForte Assure

As an integral part of its CloudForte® practice, Unisys incorporates CSPM principles and tools to comprehensively address cloud security and compliance with our CloudForte® Assure™. This product performs systematic security and compliance reviews across your hybrid and multi-cloud infrastructures, on demand. Results of the analyses lead to best practice guidance and detailed improvement plans, or, in many cases, security optimizations automatically applied.

Our CloudForte Assure tools and services cover security-compliant design, implementation, and operations of cloud infrastructure, applications, workloads, DevOps, and multi-cloud integrations. (See Figure 2).

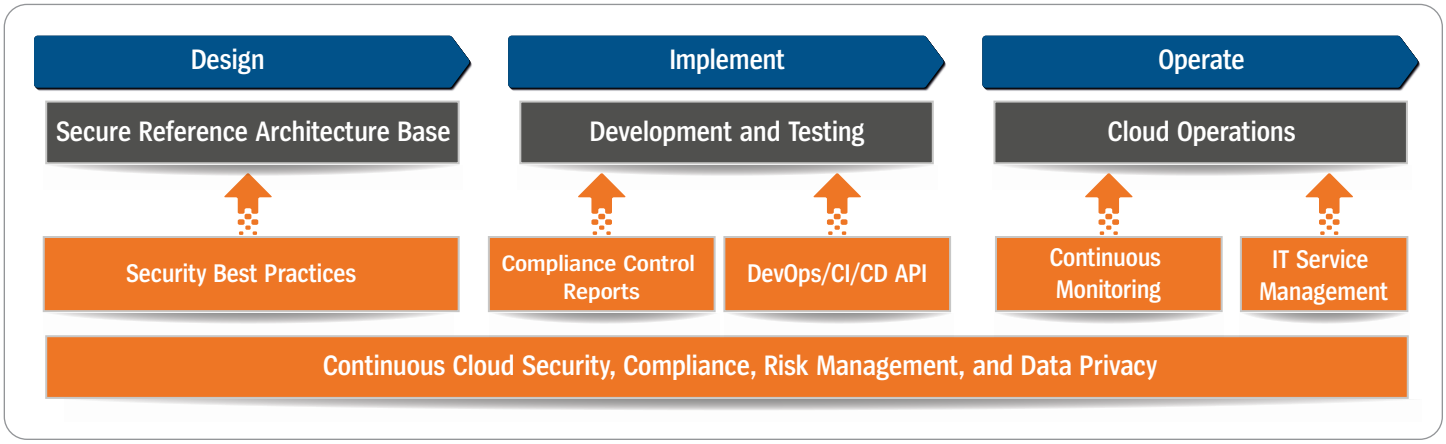


Figure 2. CloudForte Assure Cloud Security Posture Management Workflow from Design, Implementation, to Operations.

From Initial Assessment to Live Security and Compliance Monitoring

Unisys CloudForte advisors and security experts build security and compliance into every design. During our Discovery and Guided Review phase, we conduct extensive, vendor-neutral system analyses to capture the current state of existing systems and compare them to industry standards and best practices. Existing clouds can then undergo upgrades and remediation. Migration implementations begin with a complete assessment of existing legacy systems before constructing a new security architecture for the target cloud.

Move to Continuous Security, Compliance, Risk Management, and Data Privacy Assurance

The industry is already moving towards continuous security and compliance. For example, the latest PCI DSS updates recommend continuous compliance in its latest guidelines; meanwhile, NIST 800-53r4 mandates continuous security monitoring as part of their standards. Unisys is committed to providing continuous security, compliance, risk management, and data privacy through its real-time monitoring (see Figure 3).

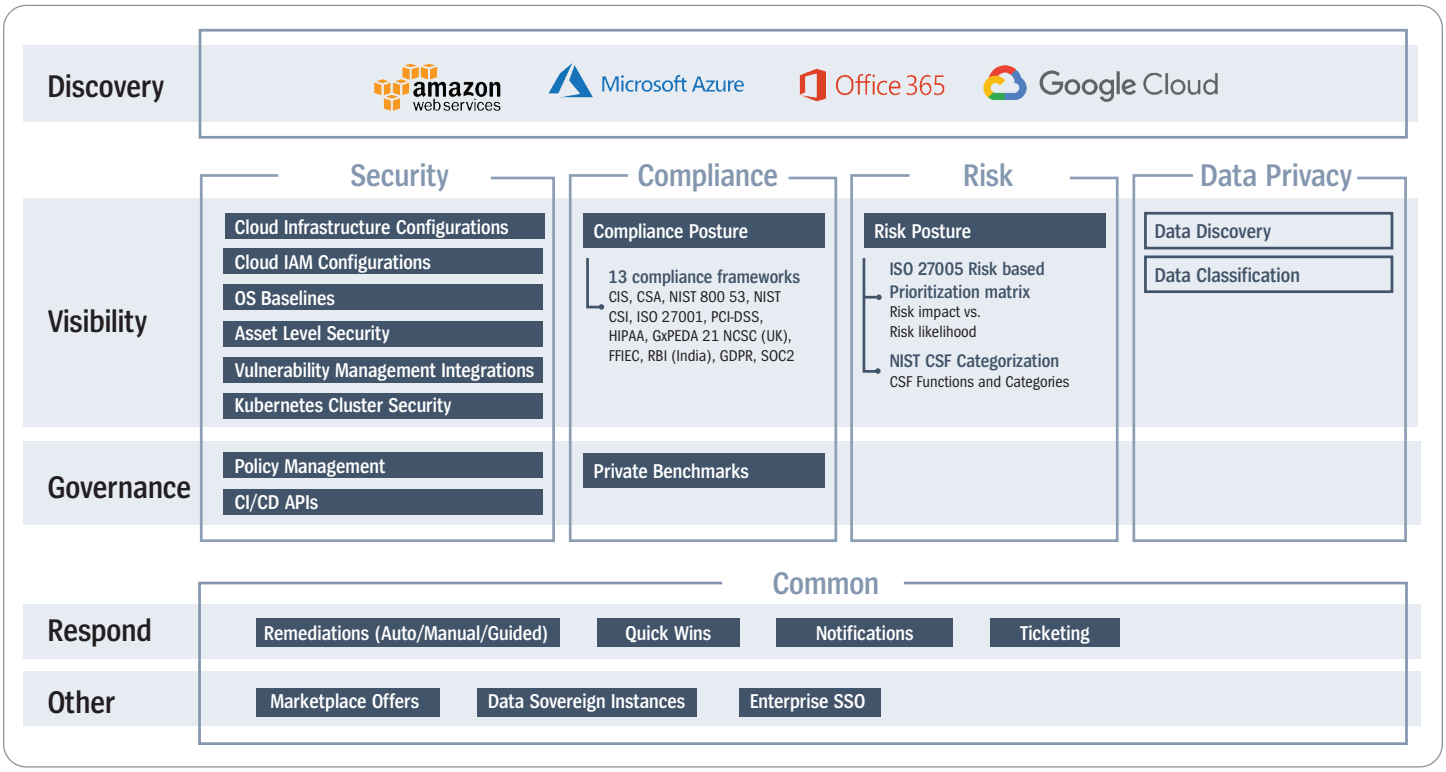


Figure 3. CloudForte Assure – Features and Domains.

Security and Compliance Through Automation

By utilizing the SaaS-based security and compliance monitoring in CloudForte Assure as a diagnostic tool, Unisys can automate many security and compliance tasks. Operations can be alerted in real time to match security and compliance variances. Guided remediation or Unisys managed services personnel can address security, compliance, risk, and privacy issues immediately. It is one of many cloud automation innovations within CloudForte.

When you select CloudForte Assure, you get the controls, processes, and automation for constant compliance improvements. CloudForte Assure integrates with customer's IT Systems to enable closed loop remediation. It enables data feeds for reporting and audit logs and integrates with ticketing systems and CI/CD automation.

CloudForte Assure Summary of Benefits

When security and compliance is built-in from the outset, cloud systems are more secure, less costly to maintain, and require fewer remediations. CloudForte Assure delivers:

- Single pane view that helps you monitor real-time security, compliance, risk posture, and data privacy information across cloud providers
- Real-time, "on-demand" security, compliance, risk, and data privacy monitoring of your entire environment
- Real-time discovery of cloud workloads to enable agile and continuous process to ensure adherence with guidelines and to identify security gaps
- Governance and remediation recommendations to fix security issues, non-compliant resources, and remediation project support
- Security management integrated into existing application development life cycles
- Top to bottom "security-optimized" environment enabled by detailed compliance reports and remediation strategies Effective, comprehensive compliance expertise for cloud from planning to implementation and operations-the entire cloud lifecycle
- Effective, comprehensive security, compliance, risk management, and data privacy expertise for cloud from planning to implementation and operations-the entire cloud lifecycle
- Controls, processes, and automation for continuous improvement
- Support and integration with DevOps and multi-cloud environments

Unisys can also provide Cloud Security Posture Management training and expertise in fostering a continuous security and compliance culture.

---

[i] Smarter with Gartner. "Is the Cloud Secure?" October 2019. https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

[ii] Thales. "2019 Global Cloud Security Study." https://cpl.thalesgroup.com/cloud-security-research

[iii] CPO Magazine. "Understanding the GDPR Cost of Continuous Compliance." May 31, 2019. https://www.cpomagazine.com/data-protection/understanding-the-gdpr-cost-of-continuous-compliance/

[iv] Unisys Cloud Barometer Survey. https://www.unisys.com/Style%20Library/Unisys/cloudbarometer/pdfs/Report_UnisysCloudSuccessBarometer.pdf

[v] Gartner. "Innovation Insight for Cloud Security Posture Management." January 2019.

To ensure continuous cloud security, compliance, risk management, and data privacy, visit www.unisys.com/CloudForte

For more information visit www.unisys.com