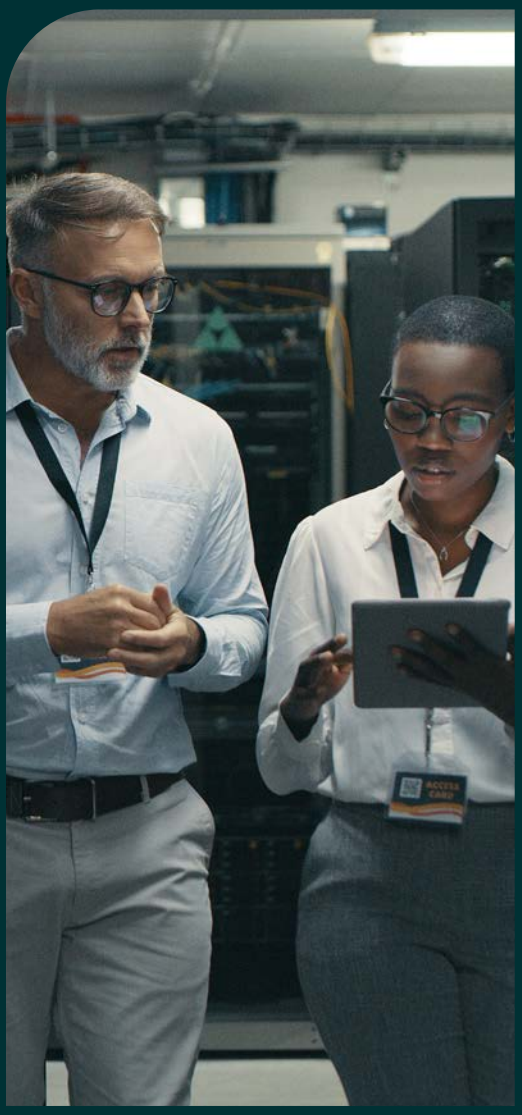
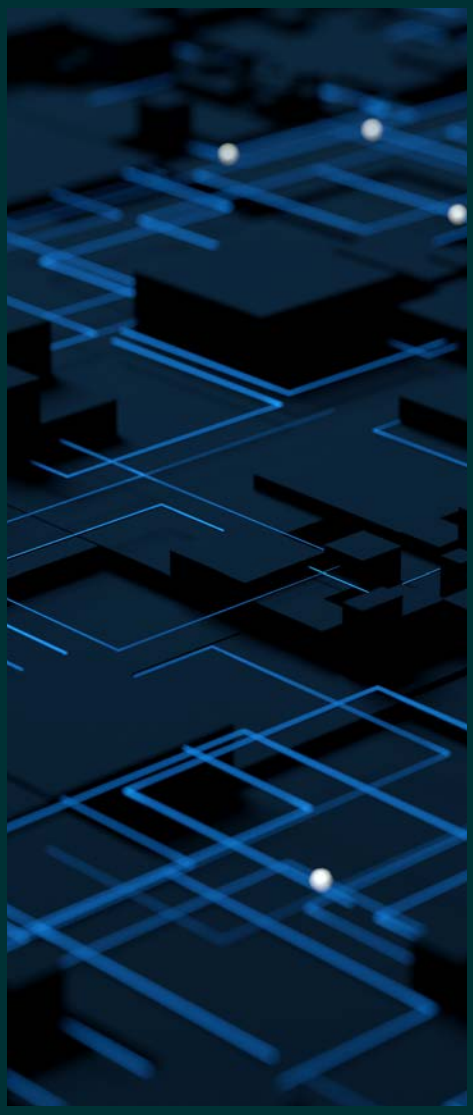
unisys

Take charge of your multi-cloud security and compliance





Multi-cloud is secure — but most deployments are not

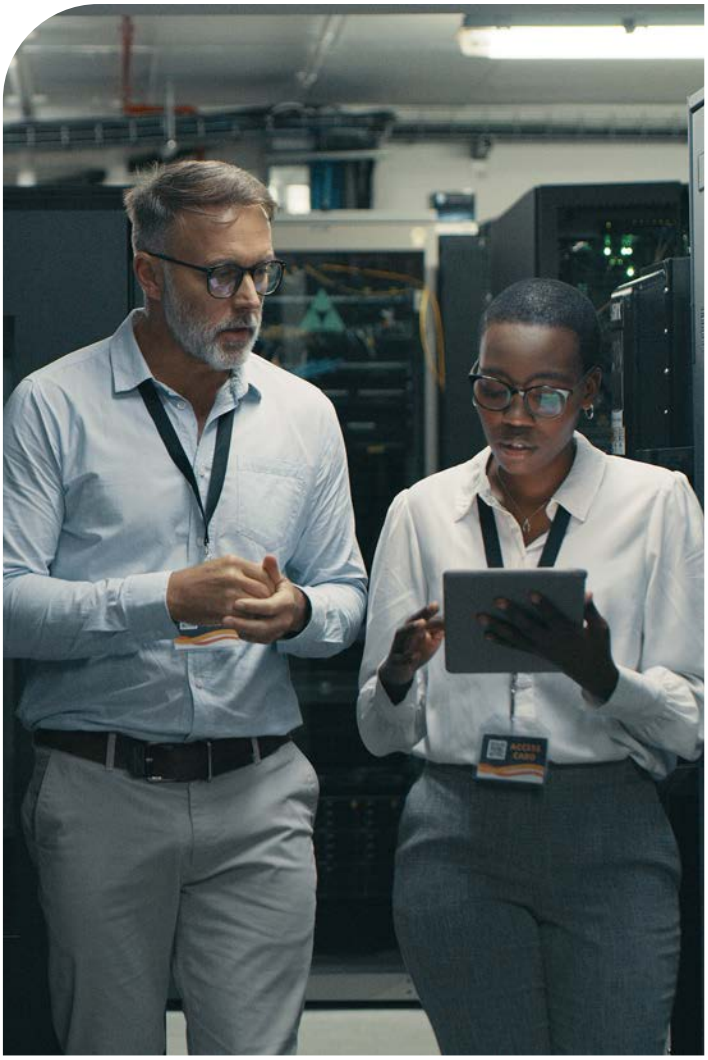
You hear a lot about cloud security lapses and high-profile breaches in the news. Industry reports and analysts exhaustively cover sensational cases publicly. But if you dig deeper into the details of these breaches, you'd discover that many of these vulnerabilities could have been avoided if the cloud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

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. Cloud needs continuous re-examination and remediation, especially in fast-paced DevOps environments.

Cloud adopters may not be fully cognizant of all current and constantly 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 governed 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 and governed continuously.

Security is also closely entwined with how cloud infrastructure is defined and used. Every component of cloud has distinct security requirements — compute, VM, storage, network, and 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 also differs 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."



Through 2023, 99% of cloud security failures will be the customer's fault.

– Gartner, CSO Online 2021.[i]

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.

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 and on an incremental measurement calendar basis.

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 4% of the firm's worldwide annual revenue, even the smallest organizations have significant incentive to comply. There are similar regulations in the United States with the California Consumer Privacy Act, which requires a whole new round of compliance checks and security audits.

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.

More than half (58%) of survey respondents are concerned about security in the cloud.

– CSA Survey, 2021. [ii]

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 shift left to enable DevSecOps. Security design, validation and compliance 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 continuous integration/ continuous delivery (CI/CD) pipelines.

By 2022, 90% of software development projects will claim to be following DevSecOps practices.

– Gartner via TechTarget 2020.[iii]

Compliance has come to the cloud. Enterprises planning a large-scale cloud migration should absolutely consider regulated workloads as part of the pool of candidate services to operate in the cloud.

– IDC PlanScape: Regulatory Compliance in Cloud Environments, 2021[iv]

Cloud security posture management

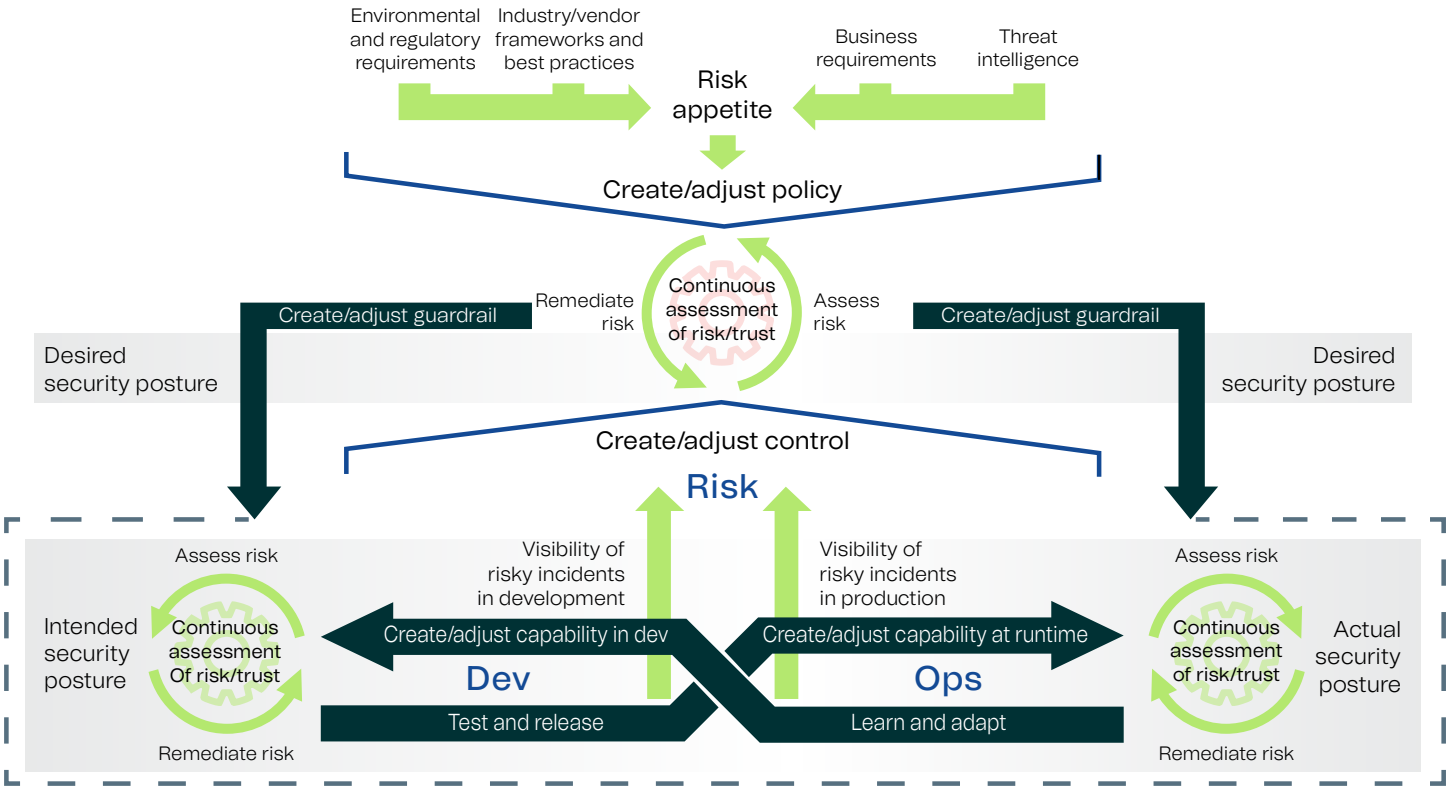


Figure 1. Cloud security posture management, Gartner[v]

A recipe for success: security and compliance throughout cloud lifecycle

A solution for ensuring security and compliance amid the rapid changes within cloud is to adopt continuous security assurance — Cloud Security Posture Management (CSPM). A CSPM solution 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, you 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).

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%.[vi]

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 your cloud environment configuration, 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, you need tools to define your minimum set of "must have" security policies for the 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 lifecycle—from its design to its deployment and ongoing operations.

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

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.

Automate security and compliance

As an integral part of its Cloud and Infrastructure Solutions practice, Unisys incorporates CSPM principles and tools to comprehensively address cloud security and compliance with the CloudForte® platform. The CloudForte Assure™ module 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.

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).

From initial assessment to live security and compliance monitoring

Unisys advisors and security experts build security and compliance into every design. During our Discovery and Guided Review phase, we conduct extensive, vendor-neutral system analysis 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. Unisys also provides Cloud Security Posture Management training and expertise in fostering a continuous security and compliance culture.

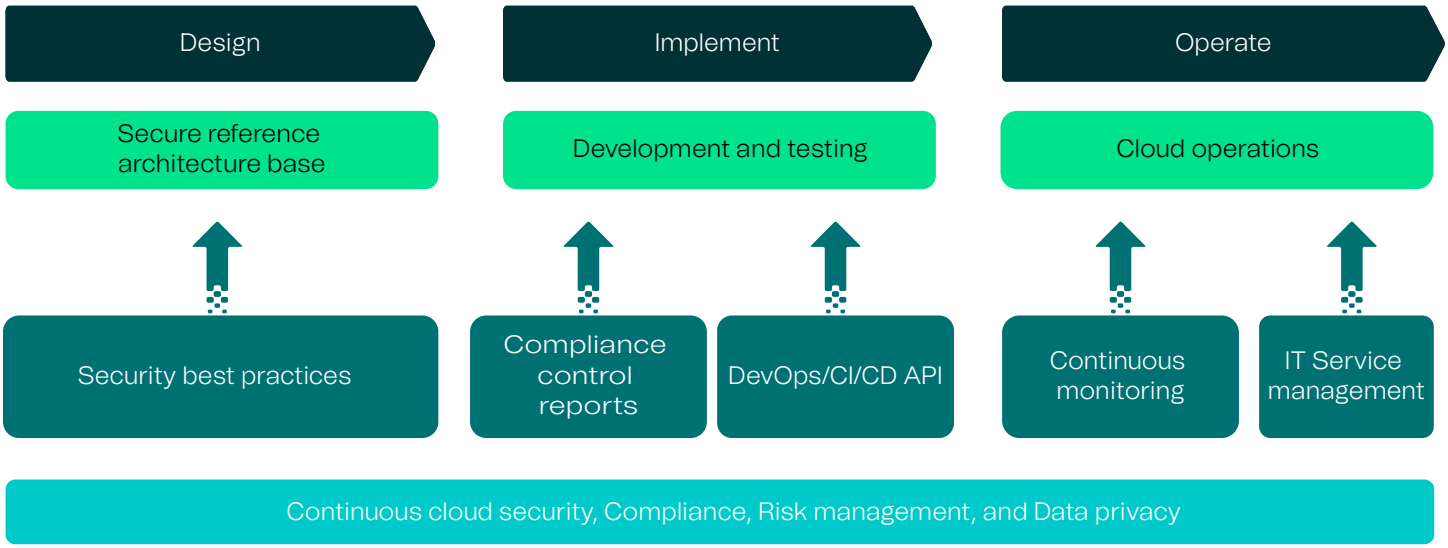


Figure 2. Cloudforte assure cloud security posture management workflow from design and implementation to operations

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 real-time monitoring (see Figure 3).

Security and compliance through automation

By utilizing the SaaS-based security and compliance monitoring in CloudForte Assure, you 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 gain an end-to-end solution that enables improved controls, measurement processes, automation, and remediation capabilities. CloudForte Assure integrates with your IT system to enable closed-loop remediation. It enables data feeds for reporting and audit logs and integrates with ticketing systems and CI/CD automation.

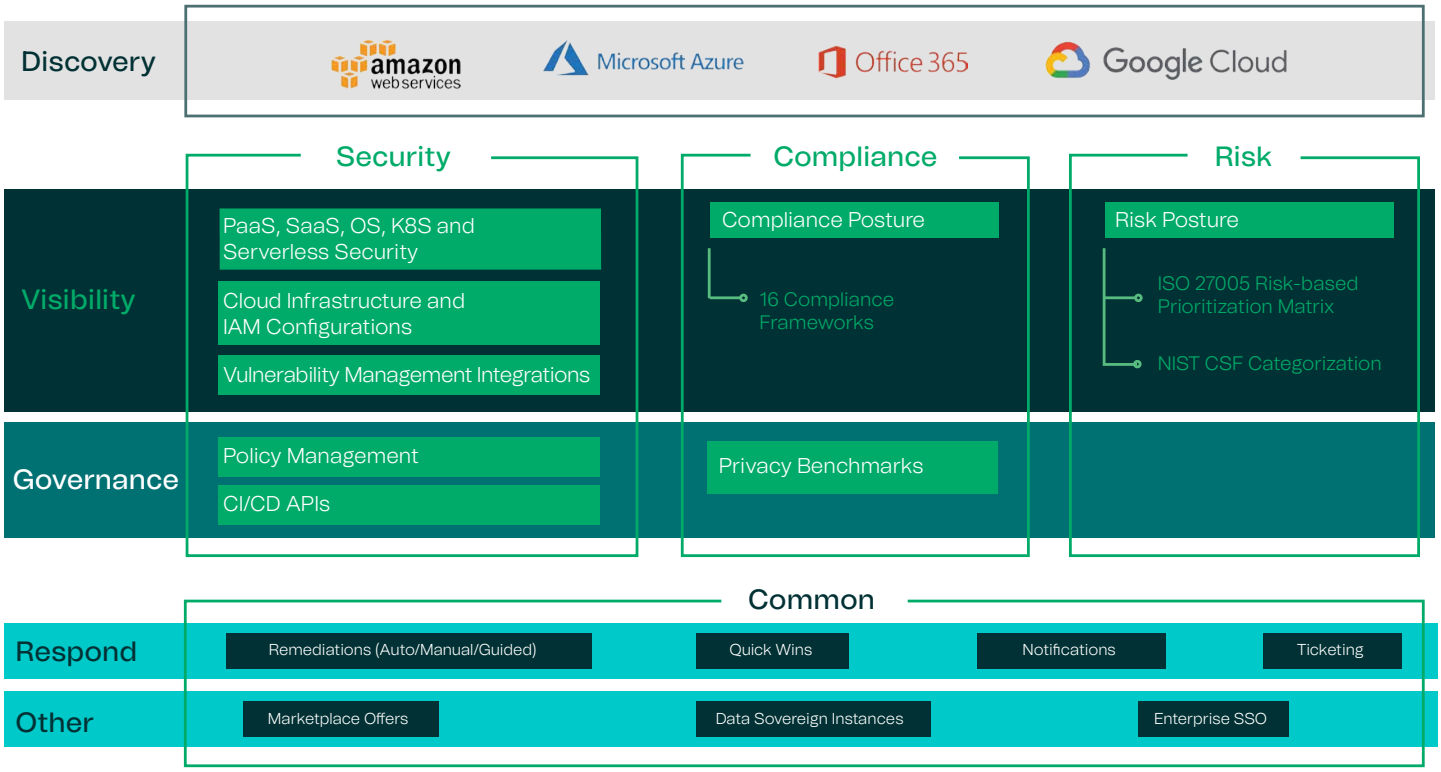


Figure 3. CloudForte assure – features and domains

CloudForte assure summary of benefits

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

- Security-optimized managed services enabled by detailed compliance reports and remediation strategies
- 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 and non-compliant resources and provides remediation project support
- Security management integrated into existing application development lifecycles
- 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
- Asset-focused views to pinpoint specific types or groups of resources for compliance and security assessment and remediation activities
- Customizable benchmarks and policies to allow tailoring to suit site-specific compliance and security policies

---

[i] SCSPM explained: Filling the gaps in cloud security, June 2021. https://www.csoonline.com/article/3620049/cspm-explained-filling-the-gaps-in-cloud-security.html

[ii] https://www.securitymagazine.com/articles/94947-csa-survey-finds-cloud-security-is-improving

[iii] https://searchsoftwarequality.techtarget.com/news/252484613/GitLab-makes-two-acquisitions-to-shift-fuzz-testing-left

[iv] IDC PlanScape: Regulatory Compliance in Cloud Environments. https://www.idc.com/getdoc.jsp?containerId=US47482220

[v] Innovation Insight for Cloud Security Posture Management, Gartner.

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

To explore how Unisys Cloud and Infrastructure Solutions can help ensure continuous cloud security, compliance, risk management, and data privacy, visit us online or contact us.

unisys

unisys.com

11/22 22-0395