Simplify and secure your cloud migration efforts

Rapid and secure large-scale migrations

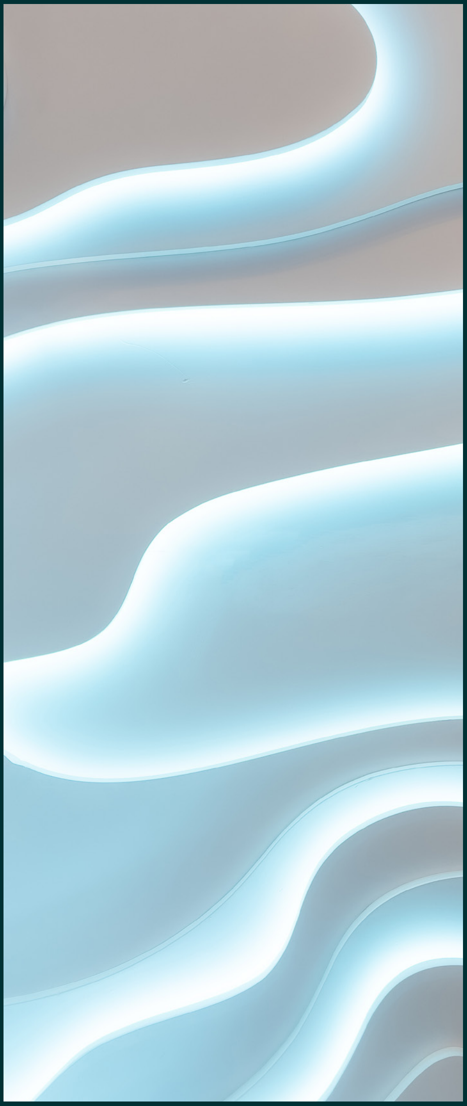


Table of contents

1.0 Cloud migration strategies 3

1.1 Large-scale, rapid, and secure cloud migration 6

1.2 Discovery, validation, assessment, and planning 7

1.3 Automated rapid migration 8

1.4 Cloud migration with DevSecOps 11

1.5 Cloud-enabled networking 11

1.6 Security approval acceleration and secure legacy workloads 12

1.6.1 Templated security control automation and secure configuration compliance automation 13

1.6.2 Secure legacy workloads with unisys 13

1.7 Unisys cloud management solution 14

1.8 Migration factory project approach 15

2.0 Summary 16

List of exhibits

Exhibit 1.0-1. Cloud migration planning options 4

Exhibit 1.0-2. Unisys cloud migration factory 4

Exhibit 1.0-3. Unisys cloud migration planning and lifecycle management approach 5

Exhibit 1.1-1. Common cloud migration challenges 6

Exhibit 1.1-2. Unisys' large-scale cloud migration approach is fully automated end to end, cost-effective, reliably secure, and supports all cloud and hypervisor platforms 7

Exhibit 1.3-1. Unisys automated cloud migration solution process flow 9

Exhibit 1.7-1. Unisys hybrid cloud management solution 14

Exhibit 1.8-1. Unisys migration factory project organization approach enables rapid and secure large-scale workload migrations 15

1.0 Cloud migration strategies

The trend is clear: If you aren't in the cloud, you are falling behind.

Cloud adoption increasingly is a key business initiative for nearly all commercial and government organizations as they strive to enable and accelerate innovation, deliver services more cost-effectively, and respond more quickly to changing conditions.

Most organizations are fully committed to integrating cloud into their IT infrastructure. According to IDG's 2020 Cloud Computing Survey:

- 92% of those polled already have at least one application or part of their infrastructure operating in the cloud
- 59% said they plan to be mostly or all in the cloud in 18 months
- 54% of applications now running in the cloud were migrated from on-prem infrastructure
- Cloud computing is expected to account for 32% of IT budgets on average over the next 12 months

For your organization to achieve genuine digital transformation, you must take advantage of the operational and cost optimization benefits of cloud-based deployments. But integrating emerging technologies can be risky and challenging. You may have thousands of legacy applications that need to be modernized and migrated in some fashion. Your ability to control costs and speed adoption are crucial factors, requiring large-scale automation and assured security, along with an imperative to keep operations up and running during the transition.

Implementing a bulk migration to the cloud requires the right partners, skills, and solutions to avoid delays and unforeseen problems. With years of assessment, consulting and transformation experience at global enterprises and governments large and small, Unisys can offer you unique insights into the appropriate path and operating model your organization should follow to migrate workloads and accelerate your move to the cloud as you seek to innovate, reduce risk, and create high-performance outcomes. As a cloud service leader, Unisys builds, manages, and secures cloud and infrastructure solutions for some of the most complex and digitally demanding enterprises and governments in the world.

A cloud migration that introduces enterprise standards will provide your organization with greater scalability, improved analytics, better utilization of IT resources and managed services, mobile and remote access, and more efficient and cost-effective disaster recovery. If you're a retail or financial organization, you can implement processes across multiple channels (storefront, digital, mobile, social) to increase revenue, improve the customer experience, and gain efficiencies. If you're a government agency, you can provide citizen services and solutions at lower costs and with greater efficiency. And whether you are a government or commercial organization, you can more quickly develop new services and products, and more easily retrofit or retire those that don't meet expectations.

There is no single, golden template for cloud migration. New applications can be developed in a cloud environment using modern cloud technology and a DevSecOps methodology. By using DevSecOps to automate software deployment, you can ensure consistent and repeatable deployments that limit the risks of introducing security vulnerabilities. You also can safely roll back deployments at any time.

For existing applications and workloads hosted in data centers, you have a number of options to consider in migrating to public clouds or private clouds, including "Lift and Shift" and container migration, which can reduce complexity while improving portability and scalability. **Exhibit 1.0-1** lists typical options for a cloud migration strategy.

Options	Description	Examples
Rehost	"Lift and Shift" move without any application platform or coding change. The compute and storage capacity may be optimized during the move. Configurations of workloads may be adjusted to the destination environment.	Migrate Windows or Linux Operating Systems hosted on virtual servers or x86 physical servers. Migrate to virtual private cloud on-prem configuration mirrored to third-party cloud provider environment for cloud native capabilities.
Replatform	For legacy applications, "replatform" migrates the applications to Windows/Linux Operating Systems or uses emulators or compatibility tools to run the applications in cloud.	Migrate mainframe applications to cloud using emulators; use AppZero for moving applications from Windows 2003 on to a newer OS in cloud; re-platform Unix applications to Linux OS and then to cloud.
Refactor	Replace some components of an application with PaaS/cloud services.	Replace an on-prem relational database with a cloud native relational database management system service.
Recode	Re-write existing applications in cloud.	Rewrite applications with cloud native services.
Repurchase	Replace the current application with SaaS solutions.	Migrate email services to Microsoft Office 365.

Exhibit 1.0-1. Cloud migration planning options

Devising a migration plan for each application system, prioritizing actions, developing the proper migration sequence, and meeting associated security and performance requirements are critical elements for your cloud migration projects. Mission requirements, business priorities, operational challenges, budget constraints, regulatory mandates, and other issues must drive the decision on migration strategy for each application.

While each cloud migration project is unique, all successful large-scale enterprise workload migrations share some core building blocks. As shown in **Exhibit 1.0-2**, these building blocks include:

- Use of a repeatable "migration factory" methodology that includes introduction of enterprise shared-service standards
- Agile-based planning/re-planning migration management
- Continuous Integration/Continuous Delivery (CI/CD), for DevOps/DevSecOps-enabled customers
- A migration management portal to track overall progress
- An end-to-end Cloud Migration Lifecycle that ensures optimal performance is maintained at the enterprise and application levels

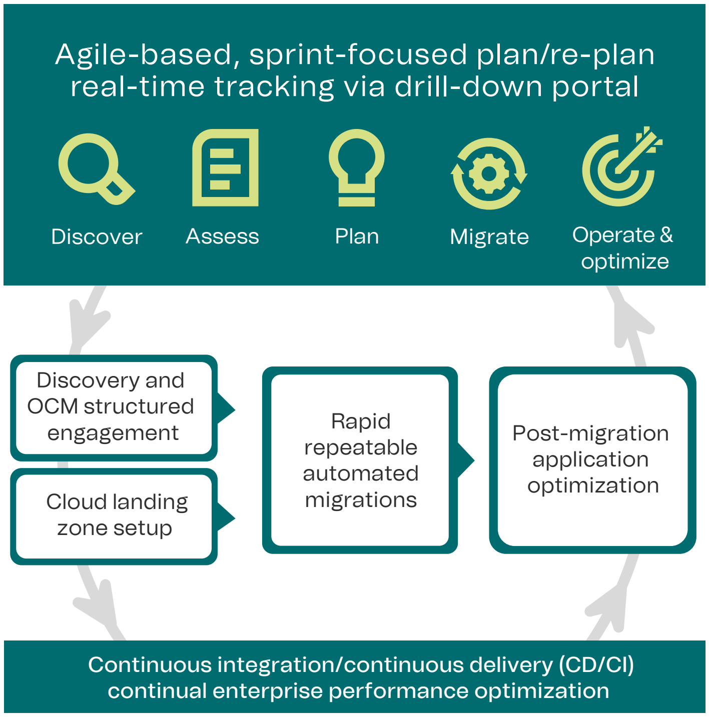

Agile-based, sprint-focused plan/re-plan real-time tracking via drill-down portal
Discover
Assess
Plan
Migrate
Operate & optimize
Discovery and OCM structured engagement
Cloud landing zone setup
Rapid repeatable automated migrations
Post-migration application optimization
Continuous integration/continuous delivery (CD/CI) continual enterprise performance optimization

Exhibit 1.0-2. Unisys cloud migration factory

If your organization has thousands of applications in its service portfolio, recoding all applications for cloud migration likely will be very time-consuming and costly. In the meantime, you still need to continue operating your data center, manage your infrastructure assets, and deal with all the capital expenditure required for refresh and capacity expansion. These challenges are more than simple annoyances. Every day that passes while locked in the data center translates into:

- **Cost inefficiency**. Costs associated with facilities, labor resources, hosting operation, assets, and hard-to-automate or -integrate operations in managing your existing data centers are unavoidable.

- **Risk with instability.** Often what drives cloud migration is an unstable facility, inadequate capacity, or lack of skilled resources in the current data centers.
- **Inability to execute.** Your organization is unable to execute against challenging environment depending on the business cycle they are currently in.
- **Unachievable speed.** You need to deliver services faster than ever before. It is an impossible task, however, when computing capacity cannot be provisioned on demand in a flexible, reliable, and elastic fashion with cost transparency.

Rapid and secure migration to the cloud can result in immediate cost savings for your organization through a reduction of facilities management, physical assets, and data center operations. Savings from data center consolidation/reduction/ elimination, efficiency in application hosting services, and transition from Capital Expense (CapEx) to Operating Expense (OpEx) then can be allocated to your application modernization. This reallocation of cost savings resolves the budget challenges facing most Information Technology (IT) organizations in IT modernization and digital transformation. The faster and more reliably that cloud migration can be performed, the higher the return on your investment.

Unisys views your cloud adoption as a journey that requires Agile-based continual assessment and optimization for improving performance, service effectiveness, and cost efficiency. As further detailed in **Exhibit 1.0-3**, we apply a structured approach with sprint-focused cloud migration planning/replanning and cloud services lifecycle management.

Our discovery, assessment, and cloud planning include detailed considerations of your business factors, people and organization, governance, applications and data assessment (including cloud suitability, interfaces, and affinity to other client applications), technical infrastructure/platform, security, and operations management. Engagement and communication with your organization is methodically planned and executed via the Unisys Organization Change Management (OCM) methodology.

Businees: Mission Benefits, Finance, Business Case, ROI

People: Skills, Knowledge, Organization, Communication

Platform: Cloud Service Provider, Architecture, Technology, XaaS

Governance: Policy and Process, EA, R&R, SDLC, SLAs, CCB

Security: Risk, Compliance, Accreditation, Architecture, Ops

Operations: ITIL ITSM Policy, Processes, and Procedures

Discover

- Applications infrastructure technology assets
- Cost
- Operations
- Stakeholders
- Dependencies
- Constraints

Assess

- Capacity and demands
- Business and service models
- App grouping
- Architecture
- Cloud readiness
- Migration strategy:
  - Rehost
  - Replatform
  - Refactor
  - Recode

Plan

- Project plan and WBS
- Resource and RACI
- Training
- Risk management
- Procurement plan
- Migration approach
- Landing zone plan
- Network connectivity
- Security plan
- Configuration and change control
- Test and QA plan
- Migration waves

Migrate

- Landing zone:
  - Accounts and IDAM
  - Network
  - Security
  - Operations support
- Pilot
- Test and validation
- User acceptance
- Communicate
- Execute cutover
- Security accreditation

Operate and optimize

- Metering and expense
- ITSM processes
- Security operations
- Monitor and reporting
- User support:
  - Configuration compliance
- Change and release
- Automate
- DevSecOps
- Cloud native solutions

Exhibit 1.0-3. Unisys cloud migration planning and lifecycle management approach.

Migrating applications and workloads to the cloud is just the first step of your cloud journey. To realize all the benefits of cloud, you must implement effective governance in security, workload lifecycle management, and expense optimization. In addition, it is imperative to leverage native services, such as Software-as-a-Service (SaaS), and Platform-as-a-Service (PaaS) available in the cloud platforms, to continually transform applications. Cloud agnostic and native cloud services provide cost-effective, innovative, flexible, and readily available building blocks for enabling bimodal IT and allowing your organization to deliver services with agility and efficiency.

Unisys provides strong expertise and service experience in modernizing mission applications with cloud-native services, and PaaS and SaaS services. Unisys worked with one large U.S. government agency to deliver many mission applications with AWS native services, including traveler identification using AWS Recognition and Lambda, and advanced data warehousing and analytics using AWS Redshift and Kinesis. For a global mining company, Unisys designed and implemented a digital transformation roadmap and migration to the public cloud of the IT infrastructure that serves more than 5,000 employees across operations spanning three continents, while producing cost savings of more than 30% by moving servers to the cloud.

A major educational institution relied on Unisys for Hybrid Cloud services, including deployment of a private and public cloud, data virtualization, and backup and disaster recovery services.

1.1 Large-scale, rapid, and secure cloud migration

You face plenty of challenges in performing cloud migrations, particularly if your environment has thousands of workloads or supports many organizations and customers.

Planned or executed improperly, your migration can be a complex and difficult operation, leading to significant efforts, cost, and risk. **Exhibit 1.1-1** highlights common challenges in migrating workloads to clouds.

Challenge	Description
Lack of complete understanding of the workloads in the source environment	Incomplete inventory of all application systems Incomplete configuration knowledge of all workloads Incomplete understanding of interdependencies among workloads and applications Incomplete understanding of the interaction and interfaces with external systems Lack of understanding/confidence on application cloud readiness
Different virtualization technologies between source and destination environments	While most IT workloads are hosted on VMware or Microsoft Hyper-V platforms, private clouds and public commercial clouds are often built with different virtualization technologies. Migrating virtual machines to a different hypervisor platform often requires ineffective manual translation and conversion.
Performance impact on production applications	Obtaining backup for systems and data in the source environment could be intrusive and resource consuming. The operation tends to degrade production performance.
Time consuming data transfer	Transferring large data and system images through WAN network can be very time and resource consuming. There is also data pilferage security risk.
Tedious and error-prone network configuration changes	Configuring network and security settings in the destination environment and preserving the original designs implemented in the source environment can be an error-prone task for large-scale migrations.
Time consuming security operating approvals	Moving applications to a multitenancy hosting environment in public or private clouds often requires security accreditation for highly regulated industries or government agencies. The Federal Authority To Operate (ATO) process, and the commercial security approvals process, can be very time consuming and costly.
Security risks with legacy systems	Legacy applications or outdated OS workloads pose security risks. In the source data center, the risks may be contained in a physically isolated security enclave. When they are migrated to a multitenancy cloud environment, a new security approval is required.

Exhibit 1.1-1. Common cloud migration challenges.

With experience delivering hundreds of global cloud migration projects, Unisys has developed best practices with a set of mature processes and proven automation solutions. We can apply our processes and automation to all kinds of workloads and all cloud platforms for accelerating the “rehost,” “replatform,” and “refactoring” migration of an overabundance of workloads to the cloud. Using our solutions, you can benefit from large-scale, rapid, and secure migration that is easily manageable, highly automated, resource efficient, and without compromise or downtime to your business operations. You will be able to simplify and automate workload migrations, ensure highly automated configuration remediation for security compliance, and deploy flexible and effective compensating security control, all while saving substantial time and generating cost savings.

As illustrated in **Exhibit 1.1-2**, Unisys cloud migration offers you effective processes and technologies to address the three major cloud migration phases: (1) discovery, validation, assessment, and planning; (2) migration; and (3) acceleration of security approvals and security protection of legacy workloads and applications that do not comply with security configuration standards.

Discover, validate, assess, and plan

1. **Discover and validate:**
   Assets, network, security, topology, dependency, application profiling
2. **Assessment:**
   App rationalization, business classification, cloud readiness
3. **Planning:**
   - app/system grouping
   - go/to-go/no-go

- Light-weight plug and play toolkit
- Checklists
- Repeatable methodology

Automated rapid migration

1. **Landing zone setup**
2. **Configuration capture**
3. **Backup**
4. **Transfer/replication**
5. **Restore and replatform**
6. **Test**
7. **Cut over**

- Automated landing zone setup
- End-to-end migration automated to any clouds
- DevSecOps process
- Rugged migration-in-a-box
- Service catalog with tiered fixed unit prices

Accelerate ATO and protect legacy workload

1. **Automated configuration remediation for compliance**
2. **Configuration security assessment**
3. **Flexible micro-segmentation for clouds**

- Secured legacy systems and distributed systems via micro-segmentation
- Automated configuration compliance scan and automated configuration remediation
- Templated security control for ATO acceleration

Exhibit 1.1-2. Unisys’ large-scale cloud migration approach is fully automated end to end, cost-effective, reliably secure, and supports all cloud and hypervisor platforms.

Unisys provides a Cloud Migration Service Catalog Manual with tiered, fixed unit prices from which our customers can order cloud migration services. In the manual, we offer fixed prices for different tiers of discovery and a migration planning service based on the size of a source data center. We offer fixed per-server migration pricing for three tiers, based on the data size and server system complexity. We offer cost transparency, service flexibility, and low project risk for our customers.

Should you need on-demand capacity to migrate your workload, Unisys offers a Core-Flex capacity model. This involves establishing the baseline team for migrating your workload at fixed cost based on the established KPIs (e.g. number of servers per month). This team can be flexed up in response to demand.

1.2 Discovery, validation, assessment, and planning

It is critical that you have a complete understanding of the inventory and interdependencies of the workloads and applications before migration. The maturity level of IT service management varies among organizations. Some IT shops have rigorous control and accurate knowledge of asset inventory, system/network/application/security configurations, application dependencies, interfaces, capacity, and performance. Other IT shops have less complete or inaccurate information. It is important to validate the inventory, configuration, and dependency information first—before beginning a migration.

Working with Unisys, you will have a highly cost-effective, high-value, lightweight solution for source data center discovery. Using our agentless discovery solution, you will be able to perform the following discoveries:

- Simple Network Management Protocol (SNMP)
- Load balancer
- Hypervisors and Virtual Machines (VMs)
- Operating System (OS)
- Domain Name System (DNS) sync and ping sweep
- Intelligent Platform Management Interface (IPMI) auto-discovery
- Services auto-discovery
- Automated application mapping
- Network and firewall topology

You also can access Representational State Transfer (REST) Application Programming Interfaces (APIs) and out-of-the-box connectors for other Configuration Management Database (CMDB) tools that exist in your environment. The Unisys solution lets you automatically build knowledge of your network environment, systems and applications, as well as the interactions and dependencies among them. And you can validate data in the source data center organization's knowledge and configuration database. In combination with application performance management tools available in your organization such as AppDynamics, New Relic, or Dynatrace, you can use the Unisys solution to build application profiling that includes application architecture, performance metrics, transaction patterns, user journey, and associated business processes.

Using a set of checklists that include triage decision trees, you can assess the cloud readiness of each workload and application based on the data acquired from the discovery activities. The readiness assessment provides one of the following outcomes: (1) ready to move; (2) cannot be moved without significant efforts to modify the application; and (3) while not currently ready for rehost migration, the workloads can be replatformed or refactored relatively easily within a short time. Unisys then plans the migration by developing workload bundles and the appropriate migration sequence. Each bundle supports a single or a set of workloads supporting applications that do not have close dependencies on systems external to the bundle.

The Unisys methodology for discovery, validation, assessment, and planning is highly automated and effectively orchestrated. Depending on the environmental complexity, a typical timeline for completing these activities is one to three months, which is far more efficient than other models.

1.3 Automated rapid migration

Your first step in executing cloud migration is to establish network connectivity, cloud landing zone, and cloud management operations for incoming workloads. Cloud landing zone setup includes:

- Setting up accounts
- Virtual Private Cloud (VPC), network and security configuration
- Identity and access management roles
- Billing and invoicing, utilization and expense management
- Governance controls
- Shared services and tools (health and capacity monitoring, security controls, backup and disaster recovery/continuity of operations [DR/COOP], event and incident management systems, and integration)

In your cloud management operations implementation, key processes are deployed and teams are mapped to support cloud management. Unisys conducts project partnership workshops with you and other stakeholders to decide tooling and configuration preferences. The Unisys solution provides you with configuration templates and automates implementation of landing zones in AWS and Azure.

With the Unisys migration solution, you can fully automate the migration process. Use it to identify inventory and grouping of systems to be migrated, handle scheduling and planning, control migration jobs and logging, track and report migration status, and provide a user portal for managing the migration. Our solution treats VMs in your destination environment as a "new computer system" and loads the operating system files and data to the new computer system with proper device drivers and configuration changes. This approach enables you to support migration of both physical and virtual servers, and all hypervisors, to all cloud platforms reliably.

As illustrated in **Exhibit 1.3-1**, you can use the Unisys software solution to perform the following automated processes:

1. **Instantiate seed VMs in your destination cloud:** The Unisys solution automatically collects detailed specifications from servers (physical and virtual) in source environment and then creates the VMs in the destination cloud accordingly. This can be done through the APIs provided by cloud orchestration platforms, or just by simply creating "seed" VMs that will be replaced by the source server configuration or desired configurations during migration.
2. **Back up the source workloads:** You can create system state and data-level backup of the source workloads in a consistent state.
3. **Move your backup files and data to the target cloud:** With the Unisys solution, you can move your backup files and data with encryption and compression to the target cloud either via network replication or by transporting in a rugged physical appliance.
4. **Restore and configure adjustment:** In the destination site, the Unisys solution lets you restore servers, applications, and data to the seed VMs already provisioned and automatically applies source configurations to overwrite the seed VMs. You can apply proper device drivers based on the target cloud hypervisors and the migrated source workload operating systems. You also can set up new network configurations according to the network settings in the destination environment. All data are loaded into the appropriate cloud storage systems in the destination site automatically.
5. **Replicate the incremental changes:** Allowing normal production operation for the workloads in the source data center during migration, the Unisys solution lets you perform "incremental sync" that captures only data changes since a prior capture. It replicates incremental changes across your network to the destination site. The replication is compressed and encrypted. This greatly reduces the time needed and the impact on your source site systems.
6. **Apply test and evaluation:** The workloads migrated to your target cloud environment can be activated for application functionality, performance, and security test and evaluation. This can be performed with your existing application testing tools and scripts.
7. **Cut over:** After completing the last batch of incremental backup and restoring the servers from the backup, the cutover is performed. The servers in your target environment are promoted to production.
8. **Perform post-cutover test and validation:** Immediately after cutover, network connectivity and application functionality and performance, your supporting services (monitoring, security, backup and DR, etc.) are tested and validated.

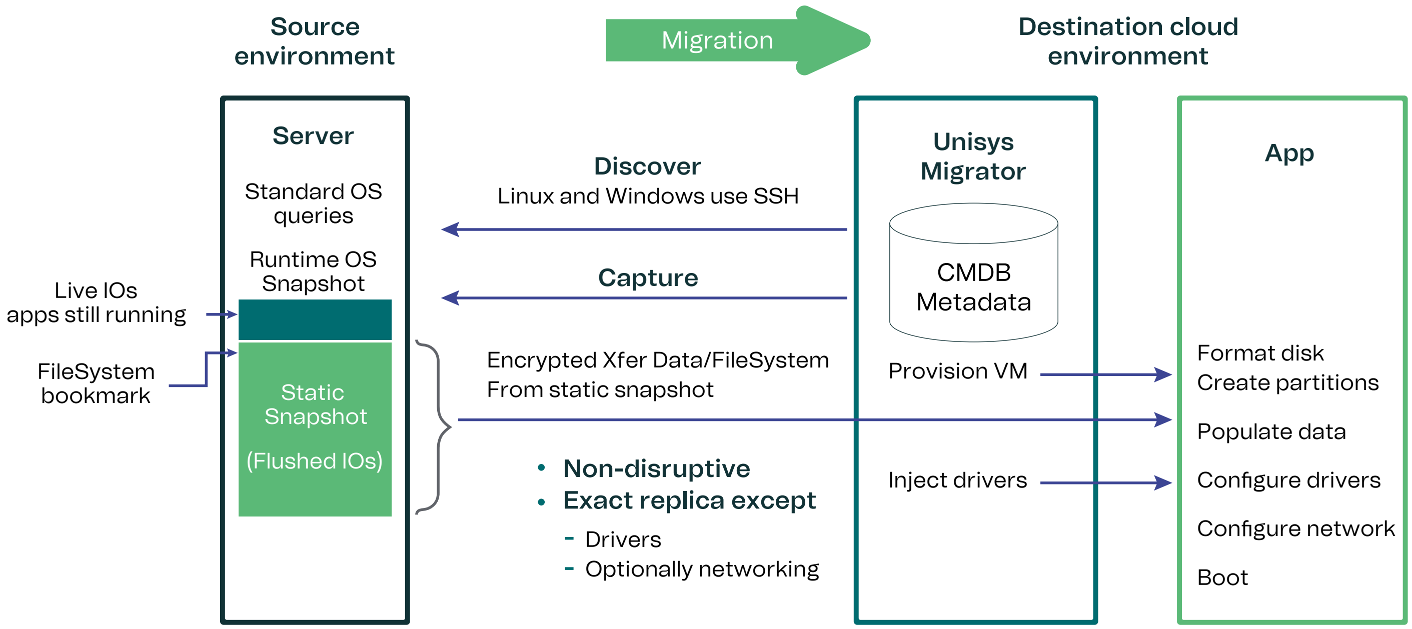


Exhibit 1.3-1. Unisys automated cloud migration solution process flow.

You can install the Unisys migration software solution as a virtual appliance in your destination cloud environment or any secure environment with secure network access to both source data centers and destination environment. It handles backup and replication across your network from source data center to the target cloud environment.

If the data and system backup size is too large for network transfer to be completed within a reasonable time, you can deploy a rugged portable system from Unisys with a form factor of flight carry-on luggage that includes compute capacity and 60+TB storage capacity. The device includes discovery software, migration software, and encryption capability. You can drop this "luggage" to a source data center for discovering and backing up workloads to be migrated, and then shipped to the target cloud data center. This allows the cloud migration of large amounts of data and large systems to be completed in a much shorter timeframe.

Other features and benefits of the Unisys solution you can leverage include:

- End-to-end migration management with an intuitive user portal that facilitates migration planning and tracks and reports status.
- Automated conversion between different infrastructure platforms:
    - Handles migrations across a wide variety of virtualization platforms automatically, including VMware, Kernel-based Virtual Machine (KVM), Xen hypervisor, Hyper-V, etc.
    - Performs automated physical server to virtual server conversion
    - Automates migration of VMware workloads to AWS, Azure, Google, Oracle, IBM public cloud, and private clouds built of CloudStack, OpenStack, Nutanix, Azure Stack, etc.
    - Automatically accounts for the features and attributes specific to a given private cloud-build technology and performs transformation accordingly
- Agentless architecture that avoids the need for you to install and manage agents in an environment with many servers. It eases operations and reduces your time, cost, and support efforts.
- Support for cloud migration testing and validation. This support allows you to stand up multiple systems in the destination site using a backup set before the final cutover.
- Customized pre-capture, post-capture, and systems standing-up operations. Scripted operations can be added to perform special actions before and after the image capture. Some examples include suspending virus scanning, putting an Oracle database in backup mode before the capture, or changing the allocation of virtual resources during migration.
- Highly efficient, resilient, and secure data transfer. All data are transferred in encrypted and compressed format and secured from tampering or data pilferage. It provides error handling and operation retry features, so intermittent network connectivity issues do not cause data transfer failure.
- Unwind logical volume management in physical systems. In private and public cloud environments, storage subsystems are typically RAID configured. The Unisys solution automatically removes the logical volume management from physical systems contained in the source site during systems conversion.
- Automated "guest software" management. Many virtualization platforms require VMs to run platform-specific "guest software" (system software and drivers) to function properly. Our solution automatically removes the "guest software" from the source site images and applies the proper "guest software" required for the destination site.
- Network configuration automation. Network environment in the destination site often differs greatly from the source site. This feature automates the network setting reconfiguration and bulk editing for you to streamline the changes.
- Right-sizing of applications. Through this process, our solution also can determine the right size of the hosting servers in memory and processing. The added benefit for you is cost savings by knowing the right infrastructure is being used.

From configuration to capture to cutover, the Unisys end-to-end migration workflow turns what would be a complex migration process with unpredictable downtime into a series of simple and repeatable steps on groups of servers. You can replace numerous manual steps and eliminate a major source of migration errors and failures, while incorporating local customizations and special cases seamlessly into the process. With the Unisys workload migration solution, you will realize the following benefits:

- Rapid and secure migration for a large quantity of your workloads
- Near-zero disruption to production during your migration
- Automatic determination and execution of the required translation and transformation at the destination site; automatic handling of complex and error-prone transformations required to get an existing system running in a new infrastructure
- Support for all cloud platforms, all virtualization technologies, and bare-metal computers
- Automated customization required before and after migrations
- Management and tracking of migrations and all stages of each migration

After your migration, your organization can benefit from support provided through the Unisys cloud factory to help you get ready for operations in the cloud environment and optimize application performance in the cloud (e.g., how to effectively use the building blocks for organizational standards that have been left during the migration).

1.4 Cloud migration with devsecops

Using the Unisys migration solution, you have the option to perform rapid and secure cloud migration with DevSecOps methodology and toolchains. This is a solution we provide to customers who have adopted or started to adopt DevOps or DevSecOps continuous integration/continuous delivery (CI/CD).

With this approach you can deploy configuration and orchestration management solutions, such as Puppet, Chef, Ansible, Terraform, etc., to capture the infrastructure system and application configurations in the source data center and then deploy the configurations and data to the target cloud environment in the form of VMs, containers, or cloud-native services using DevSecOps methodology.

You can use CI/CD tooling for application performance monitoring, test automation, configuration management, code vulnerability scanning, Section 508 testing, build repositories, and open source governance tools. You also can port the application artifacts (source code, test suites, build automation, test data, deployment automation) to the CI/CD toolchain. Landing zone templates can be used as part of your continuous delivery automation phase and incrementally build out a set of “infrastructure as code” artifacts in a time-boxed iterative manner.

This automation ensures your application and associated content can be automatically and repeatedly (re) deployed with integrated regression, performance, and security scanning tests. You can leverage CI/CD tools that support dashboard (such as SonarQube) to automate the display of the current code quality and security quality of the application. The automated display minimizes the risk of out-of-date assessment documentation. With the Unisys solution, you have access to API management tools, such as Swagger self-document APIs, to ensure documentation is up to date.

By applying the DevSecOps toolchain, you can automate cloud migration and continuous delivery of cloud applications. The choice of specific tools for your initiatives will be driven by many factors, including the consideration of tools you already deploy and use, standards and architecture, the unique requirements for migration, etc. You can make these decisions collaboratively with Unisys early in the cloud migration initiative.

1.5 Cloud-enabled networking

Virtualization of data center assets and growing reliance on cloud services are redefining the nature of enterprise-class networking. As your organization places more of its workloads in public cloud services and adopts private cloud environments to serve the most critical business applications, you migrate away from hardware-based legacy networking models to software-defined networking models that accommodate your bandwidth, flexibility, and performance needs.

Your move to the cloud is not complete without cloud-enabled networking. This extends your network, at any data center gateway, with a secure private connection that enables a scalable and robust multi-cloud networking infrastructure that delivers virtual instances of compute, storage, and network resources catering to both your public cloud services and business-critical private cloud applications.

Optimizing networks and data centers for cloud environments requires updated technologies. Enterprise networks rarely are built for the amount of LAN traffic that will be pushed to the Internet when the most-used applications are in the cloud. Improvements often are needed at the gateway, Internet connections, and traffic routing from satellite offices. When this concern is left unaddressed, users can experience latency and connectivity issues that originate at the enterprise.

According to Network World's 2020 State of the Network survey, 46% of surveyed organizations plan to add software-defined networking to their modernization strategy, and 20% already have SDN in place. SDN "allows the network to direct traffic without relying on the hardware to make the decision and positions organizations for new technologies, including IoT devices, cloud-based applications and big data apps," Network World writes.

The new data center needs a scalable and robust multi-cloud networking infrastructure that delivers virtual instances of compute, storage, and network resources catering to several business-critical applications. However, these technologies must integrate and interoperate across data centers and applications that reside in various clouds. Your organization must adapt to provide a safe, robust connection to business-critical applications and data while seamlessly enabling business users to leap into a fully digitized workspace.

Many service providers offer SDN, Network Virtualization, and Infrastructure-as-a-Service (IaaS). But only a select few service providers like Unisys combine these services from various providers and deliver them as a single entity, eliminating the various interoperability and management issues that may occur if those services are delivered individually.

With a cloud-enabled network solution from Unisys, you benefit from a seamless and secure connection across the WAN to remote data centers supporting both on-site and mobile connectivity. You enhance your network availability and security by offering dedicated connectivity from Unisys hosted secure data centers using Multiprotocol Label Switching (MPLS) networks, a Peer-to-Peer (P2P) Ethernet network, or cross-connects at our facilities.

Using the Unisys solution, you further strengthen your organization's IT environment by simplifying management for the entire multi-cloud infrastructure through a single pane of glass.

1.6 Security approval acceleration and secure legacy workloads

For U.S. Government customers, achieving security Authority To Operate (ATO) is required for all systems operating in a production environment. Achieving an ATO is often a difficult and time-consuming process. Non-Government customers frequently have similar time-consuming security approvals to allow operations in their production environments.

Even for rehost migrations, while there are no application changes, the security controls in the destination cloud environment still need to be set up and configured properly to meet assessment and accreditation requirements. Application updates/upgrades over time often lead to some deviation from the secure configuration compliance requirements and cause the security approvals for cloud migration to become a challenging issue that can cause long delays.

In addition, for legacy workloads (i.e., old operating systems, outdated software applications that cannot be patched) and specialized applications that cannot be patched easily (i.e., industrial control systems, medical control applications, Enterprise Resource Planning [ERP] applications, scientific research applications), security compliance is a challenge when migrating to a multitenancy cloud environment. There are situations where applications need to be deployed across clouds and on-prem data centers in a highly distributed architecture that is hard to secure.

To address these challenges, Unisys provides two distinct solutions: 1) Templated security control automation and secure configuration compliance automation; and 2) Security software that provides a compensating security control to protect legacy or distributed workloads.

1.6.1 Templated security control automation and secure configuration compliance automation

Unisys offers preconfigured, templated security control solutions based on your organization's security compliance requirements. Our solution automatically deploys required security controls and proper environmental configurations. It reuses and inherits the controls already authorized in the cloud compliance packages. We use landing zone to isolate the controls to be addressed uniquely for each application in the migration. Our automation solution scans configuration compliance and applies security remediation for all workloads. It automates the creation and maintenance of secure, compliant environments specific to each application.

1.6.2 Secure legacy workloads with Unisys

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. With the Unisys security solution, you can implement continuous, real-time security posture management and regulatory compliance best practices for your cloud and multi-cloud environments.

You can secure your communities of interest from attacks by using the Unisys software-defined security solution that applies user identity, role-driven micro-segmentation, and AES-256 encryption to protect data in motion. Our solution leverages role and identity of users and workloads, not by Internet Protocol (IP) addresses, to build security policies. It implements and manages a least privilege/zero trust model based on identity and provides you with a unified security platform that can extend across the enterprise—cloud, data center, and mobile. Our solution is a National Security Agency (NSA) Commercial Solutions for Classified (CSfC) certified solution. It can be deployed over any network transports (physical or virtual) and effectively prevent unauthorized east-west network movement.

You don't need to reconfigure systems or applications with the Unisys solution, which is easily integrated into existing infrastructure with minimal disruption by virtualizing network topology—dramatically reducing your security management complexity and cost. You can integrate the Unisys solution with cloud infrastructure and the solution can deliver protection to critical workloads across public and private clouds. It also allows organizations to quickly gain insight into network relationships and suspicious communication.

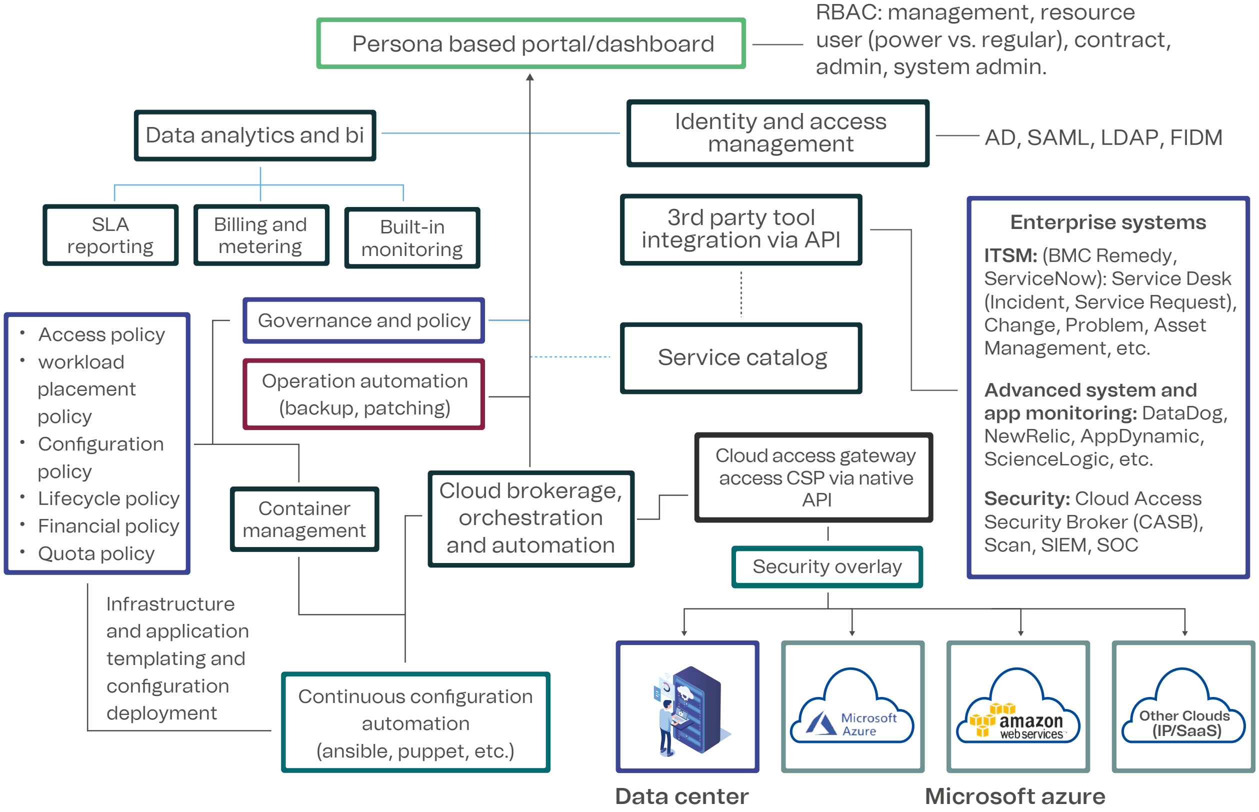
Using heuristic analysis of network data, the Unisys software provides visibility into network trespass attempts and traffic, taking preventive actions to quarantine the risks. It provides intuitive traffic flow visualization that enables policy modeling to allow an organization to determine how best to permit, restrict, or block communications between sensitive data and unauthorized users. It also allows dynamic policy and controls adjustment on the fly to align with business and regulatory requirements. The benefits of the Unisys security solution for a cloud environment are:

- Preventing lateral movement of unauthorized users on your cloud network
- Minimizing exposure through identity-defined, securely encrypted communication
- Protecting legacy systems and workloads by reducing attack surfaces and confining user access and application traffic within a secured logical enclave
- Operating secure distributed applications across your public and private cloud environments
- Providing dynamic micro-segmentation and quarantine threats in seconds vs. days or months

Unisys is an NSA Trusted Integrator, and our CSfC security solution supports any desired segmentation with highly flexible configurations. You can rapidly apply it to your target workloads and applications without any hardware purchase and deployment. The solution provides the security assurance to application owners and cloud hosting operators and enables a rapid and secure cloud migration.

1.7 Unisys Cloud Management Solution

Successfully completing workload migrations or application refactoring/recoding to the cloud is only half the battle. You still need to implement a cloud management service to ensure best practices are in place for enterprise-level service management, utilization and expense management, governance, and security. With Unisys, you can deploy multiple cloud management solutions for managing either hybrid cloud environments or public clouds according to your needs. Our integrated cloud management platform solution is described in **Exhibit 1.7-1**.



Persona based portal/dashboard
RBAC: management, resource user (power vs. regular), contract, admin, system admin.
Data analytics and bi
Identity and access management
AD, SAML, LDAP, FIDM
SLA reporting
Billing and metering
Built-in monitoring
3rd party tool integration via API
Enterprise systems
ITSM: (BMC Remedy, ServiceNow): Service Desk (Incident, Service Request), Change, Problem, Asset Management, etc.
Advanced system and app monitoring: DataDog, NewRelic, AppDynamic, ScienceLogic, etc.
Security: Cloud Access Security Broker (CASB), Scan, SIEM, SOC
Access policy
workload placement policy
Configuration policy
Lifecycle policy
Financial policy
Quota policy
Governance and policy
Operation automation (backup, patching)
Service catalog
Cloud access gateway access CSP via native API
Container management
Cloud brokerage, orchestration and automation
Security overlay
Infrastructure and application templating and configuration deployment
Continuous configuration automation (ansible, puppet, etc.)
Microsoft Azure
amazon web services
Other Clouds (IP/SaaS)
Data center
Microsoft azure

Service federation and integration

- IT team autonomy with enterprise compliance
- Centralized management and reporting

Tiered governance

- Customized, multi-tier policy engine
- Ensures compliance and responsible consumption

Flexible self and managed service

- Self-service guardrails at policy/tier/role level
- Flexible managed service options

Native cloud services

- Multiple clouds: AWS, Azure, Google, IBM, private cloud
- Native cloud services (pre-integrated, and gateway options)
- Quick extensible to new cloud/services

Adaptable cost mapping

- Ingests CSP costs, reports by client cost centers
- Intuitive tagging/mapping to link CSP to client

Container support

- Point-in-time visibility to containers (API enabled)
- Policy-based container security

Packaged application deployment

- Drag-and-drop build of blueprints for complete systems
- End-to-end assembly of application system components

Automated, template-based installation of compliant environments

Secure cloud solutions

- Well-architected, secure solution consisting of cloud-native workload deployments and ancillary tooling for ongoing monitoring, policy-driven management and optimization

Exhibit 1.7-1. Unisys hybrid cloud management solution.

Unisys cloud management solutions empower you to leverage a well-architected framework for modernizing legacy infrastructure applications. You can conduct continuous assessments with remediation guidance on the best architecture and recommendations for migrating to the cloud and transforming applications. Infrastructure and application modernization guidance helps you update legacy software for modern business needs. You can review Kubernetes security against best practices to ensure secure cloud deployment, management, and auto-scaling. And you can take advantage of Unisys partners such as Morpheus Data, which provides a powerful self-service engine for managing hybrid clouds and modernizing apps.

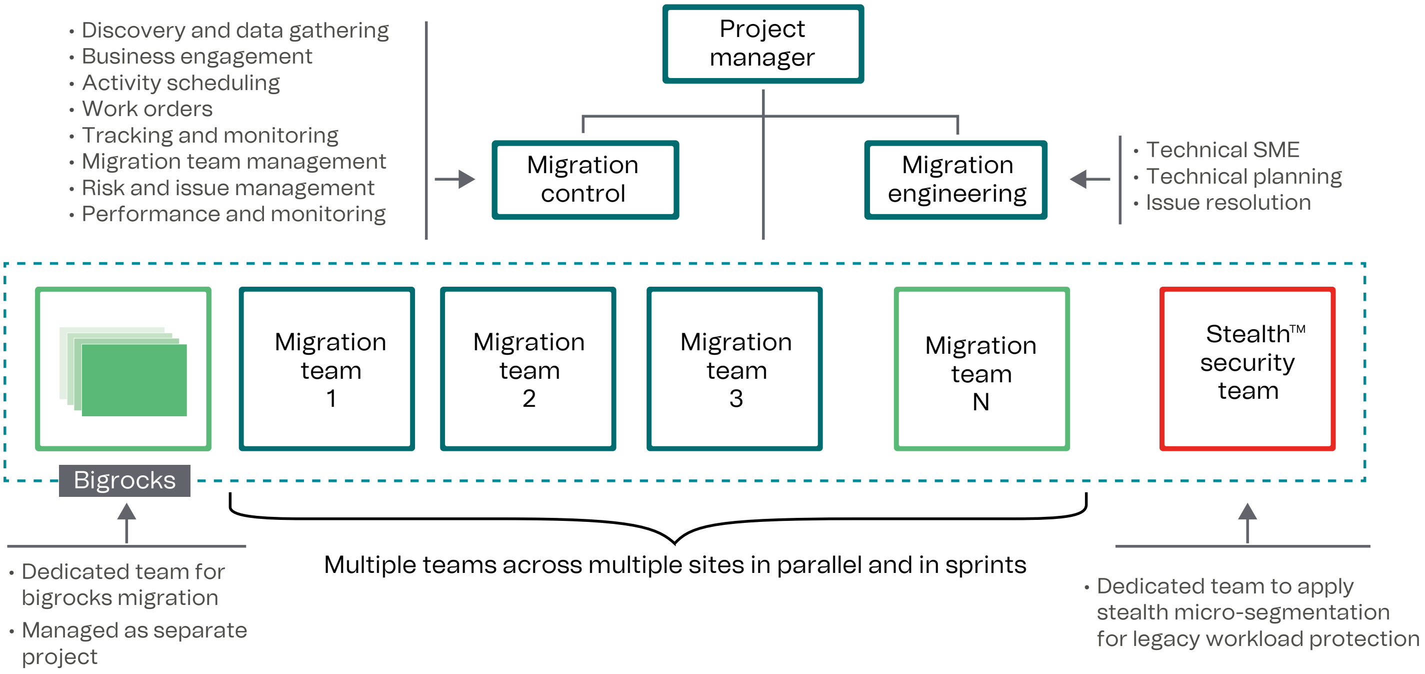
You also can save money with the Unisys approach to cloud cost optimization. Even if you are able to successfully complete large-scale migrations, you may struggle to control costs over time as you accumulate overprovisioned or idle resources. With Unisys you can find significant cost savings across hybrid and multiple clouds by monitoring your cloud spend, driving organizational accountabilities, and optimizing cloud efficiencies. Cloud cost reporting and optimization will reduce your overall cloud spend by identifying mismanaged resources, eliminating waste, reserving capacity for higher discounts, and right-sizing computing services to scale. Using the right tools and processes, Unisys customers have seen an average reduction in cloud costs of 30%. Some customers have saved up to 60% by implementing our cost optimization practice.

This is a highly scalable cloud management platform solution that provides you with multi-level governance, persona-based portal, automated application provisioning across all cloud environments, cost optimization, centralized service management and governance, a validated reference architecture, micro-services management, advanced analytics, and direct access to native cloud services with overarching governance.

1.8 Migration factory project approach

In delivering cloud migration services, Unisys applies our migration factory project approach that enables you to perform migrations across multiple workload bundles or multiple data centers in parallel. As illustrated in **Exhibit 1.8-1**, our migration factory concept of operations performs migrations in Agile sprints in a highly repeatable manner across multiple sites.

The migration factory project approach breaks down your migration into waves or phases in which servers, databases, and any other components for a group of applications can be moved to the cloud. Unisys creates parallel workstreams and forms teams (called squads). Each wave can include multiple squads for server migrations, databases, etc. This process can be repeated with subsequent waves until completion of the migration.



Project manager
• Discovery and data gathering
• Business engagement
• Activity scheduling
• Work orders
• Tracking and monitoring
• Migration team management
• Risk and issue management
• Performance and monitoring
Migration control
Migration engineering
• Technical SME
• Technical planning
• Issue resolution
Bigrocks
Migration team 1
Migration team 2
Migration team 3
Migration team N
Stealth™ security team
• Dedicated team for bigrocks migration
• Managed as separate project
Multiple teams across multiple sites in parallel and in sprints
• Dedicated team to apply stealth micro-segmentation for legacy workload protection

Exhibit 1.8-1. Unisys migration factory project organization approach enables rapid and secure large-scale workload migrations.

2.0 Summary

With years of transformation experience at global enterprises and governments, large and small, Unisys has unique insight into how your organization can accelerate the move to the cloud as you seek to innovate, reduce risk, and create high-performance outcomes. Unisys consults on, builds, manages, and secures cloud and infrastructure solutions for some of the most complex and digitally demanding enterprises and governments in the world.

Large-scale cloud migration can be a complex and difficult operation if planned or executed improperly. With the Unisys solution, you have the tools to ensure a successful large-scale, rapid, and secure migration that is easily manageable, highly automated, and resource efficient.

You will be able to simplify and automate workload migrations, provide highly automated configuration remediation for security compliance, and leverage flexible and effective security control, while saving substantial time and realizing cost savings.

Unisys provides proven technologies, methodologies, processes, and expertise for large-scale cloud migration with desired speed and security. Regardless of the type of your cloud and destination, our end-to-end fully automated cloud migration solution empowers you to move workloads to the cloud in a managed, expeditious, and secure manner with near-zero down time and risk, realizing high return on your investment.

Unisys recognizes the challenge is not in hosting in the cloud, but in the effort required to prepare applications for migration. Our solutions address the full lifecycle needs of your cloud adoption and cloud service management. Unisys expertise in applying native cloud services, PaaS, and SaaS solutions to modernize applications and transform IT services allows you to maximize the value of cloud adoption.

To find out more about Rapid and Secure Large-Scale Migrations, visit www.unisys.com/solutions/cloud-applications-and-infrastructure-solutions/#solutions.

Unisys: a cloud service leader

- Ranked by IDC as one of the Top 4 leading system integrators serving Federal Government
- Rated as a Leader in Cloud Infrastructure Migration and Management by NelsonHall and Forester in 2016 and 2017
- Rated as a Leader in the NelsonHall Vendor Evaluation and Assessment Tool (NEAT) Cloud Advisory Assessment and Migration Evaluation 2018
- Rated by Gartner as one of the three top providers having the most comprehensive strengths in Hybrid IT Infrastructure Management and Cloud Migrations
- Awarded Most Innovative Company in 2017 by Washington Technology magazine's Industry Innovators
- More than 1,300 AWS, Azure, or Google certifications

unisys

unisys.com