beacon

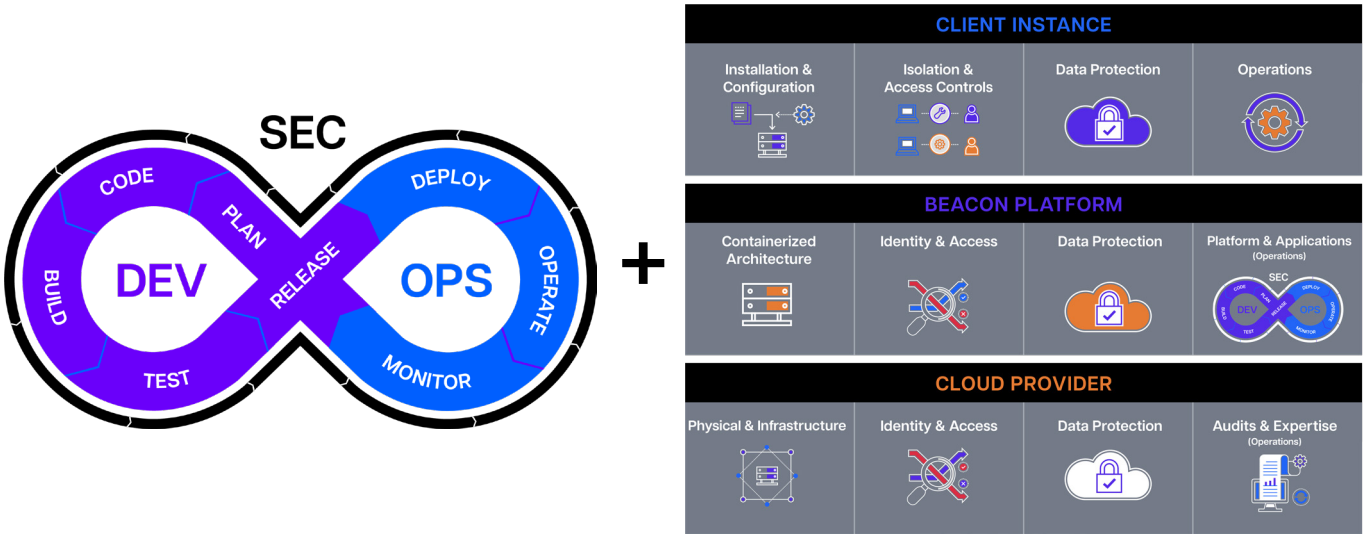
Beacon White Paper

# Beacon Cloud Security

## Reviewing Beacon's Model for Secure Development, Deployment, and Operations

# Beacon's Security Model

Protecting the information and intellectual property of our clients is an essential part of Beacon's products and services. As a developer of cloud-native tools and applications, Beacon has invested in leading security measures at every point of the platform's development, deployment, and operations. Security in the cloud has some key differences from security in data center or on-premise operating models.




Beacon's security model has two distinct elements that span product planning through client operations, and work together to deliver the highest levels of protection:

- Secure software development lifecycle process, based on DevSecOps methodologies
- Shared responsibility model for cloud infrastructure and operations with secure installation and isolation of each customer's operating instances described in this paper

This paper summarizes the essential attributes of these two security elements.

# Security Objectives

The overall objectives of the Beacon's security model and programs are to:

- Protect the company and its customers from information and physical security risk through the right mix of people, processes, and technology
- Proactively prepare for, monitor, manage, and respond to threats through comprehensive and coordinated plans
- Adapt to the changing landscape of security threats with both tactical and strategic goals
- Identify and raise significant security risks for appropriate oversight and remediation, as and when necessary

# Regulatory and Compliance Requirements

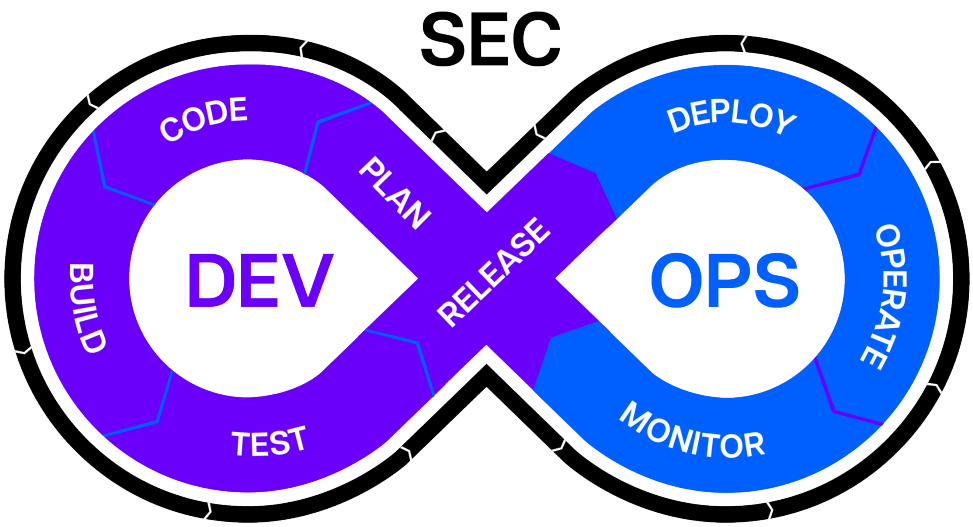
Although Beacon Platform is not a regulated entity, many of its clients are.
The company's security program is designed to align with general regulatory requirements of a variety of entities and standards, such as:

- New York State Department of Financial Services 23 NYCRR 500
- United States Securities and Exchange Commission Regulation Systems Compliance and Integrity (Regulation SCI)
- System and Organization Controls (SOC) Report 1 and 2

The overall security program is based on the Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook.

# Secure Software Development

Beacon employs secure software development life cycle processes, based on DevSecOps methodologies. DevSecOps (Development, Security, Operations) is the practice of treating security as an integral part of and shared responsibility throughout the entire software development lifecycle. More than just tools and techniques, DevSecOps is a combination of culture, processes, and technologies that create a continuous cycle of security awareness. Surrounded and enabled by a secure environment, these steps rely on clearly defined workflows and process automation to consistently deliver secure, quality code.




DevSecOps begins with continuously evaluating and strengthening the development and operating environment. This includes identifying and monitoring all relevant assets, authorized individuals, and vulnerabilities, and implementing appropriate security practices. Access to Beacon's development environment is centralized and secured with strong identity verification, authentication, and access control services for all users, with concentric circles of access. Role-based access controls use a least privilege approach for developers, limiting them to their areas of responsibility and expertise. In addition, internal systems access uses private IP addresses and a whitelist of trusted devices, severely limiting the risk of security breaches or external tampering.

Many of the company's DevSecOps processes are supported and automated by Beacon's integrated development environment (IDE), which is based on Visual Studio Code (VSCode). Standardization and automation of development and deployment workflows enhance compliance with best practices, company controls, and regulatory requirements.

# Security Architecture

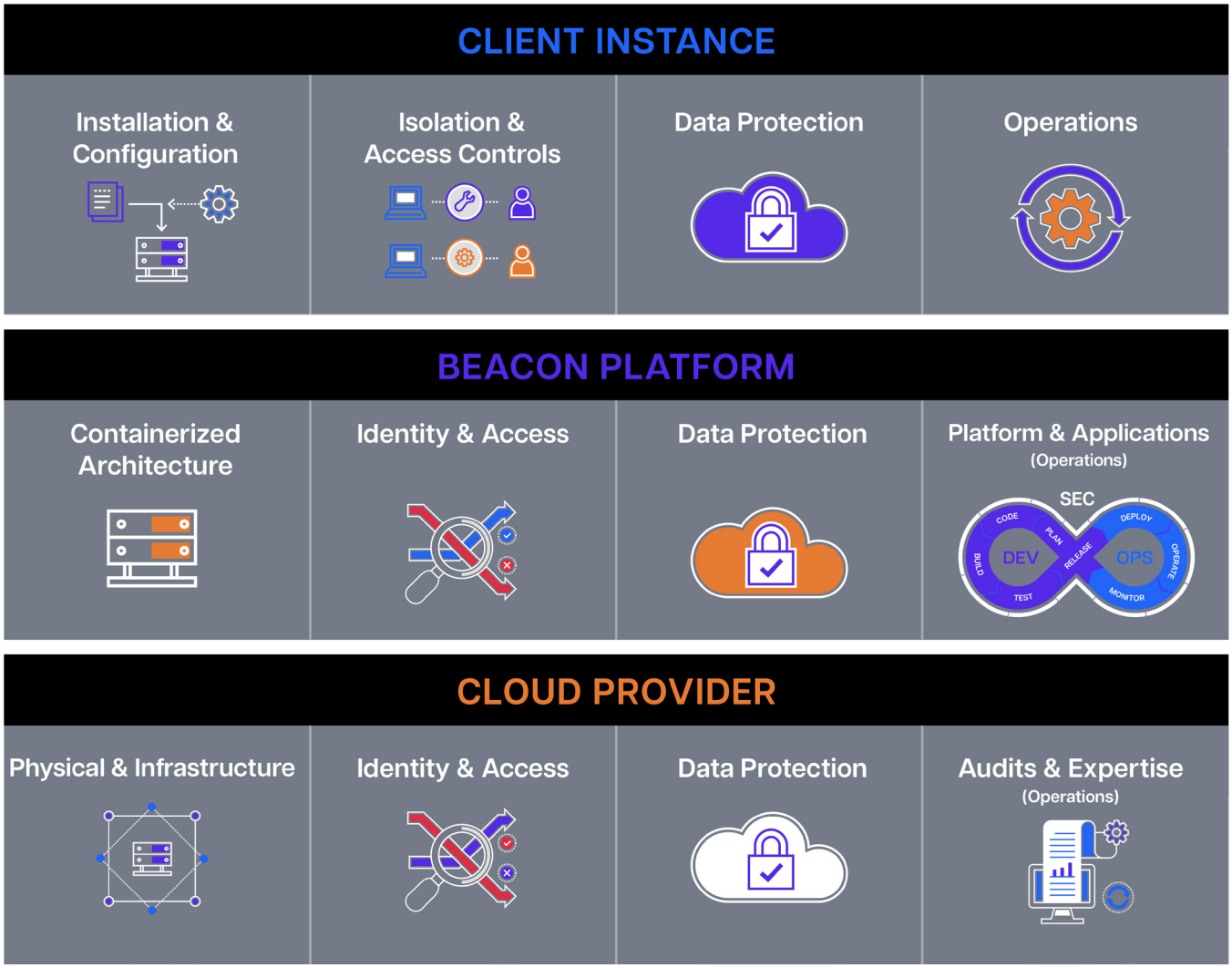
A comprehensive security architecture is an essential part of developing secure code. Beacon's secure platform development framework incorporates and translates the company's policies into specific and executable models, practices, and processes that developers and testers can readily refer to. Some key elements of Beacon's security architecture include:

- Layered, containerized architecture that isolates each workload and enables easy sandboxing
- Containers and control plane use least privilege and do not run with root authority
- Using a reduced footprint for all containers to limit the attack surface
- Automated configuration templates for containers that are maintained through a version control system to increase consistency and reduce the risk of manual errors
- Separation of code and data, encrypted data transfers, and isolation of each customer's data and processing
- Issue tracking and management tools, populated from security monitoring, threat assessments, internal testing, and customer reports
- Rapid and safe rebuild of workloads in case of suspected compromise

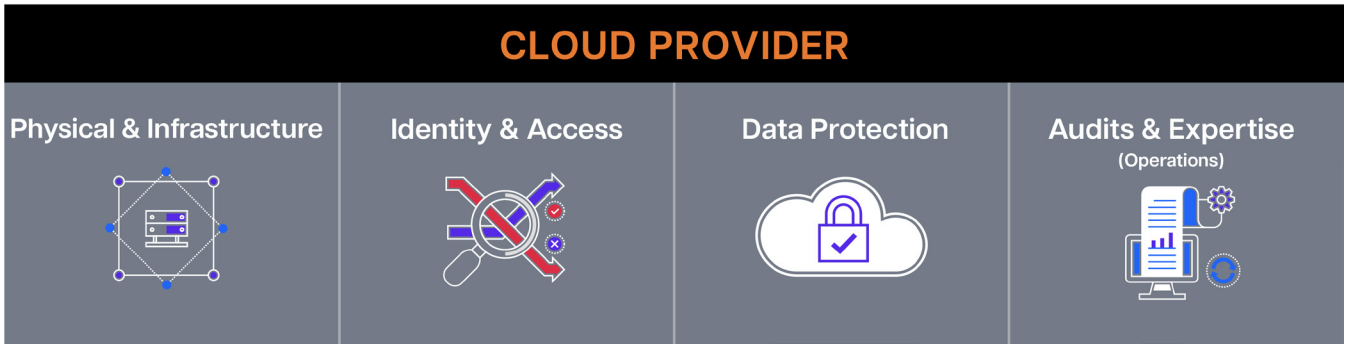
For more information, download the white paper Building Secure Systems with DevSecOps.

# Cloud Infrastructure and Operations

Beacon is a cloud-native platform that builds on the scalability and flexibility of cloud computing and data infrastructure. Security in this environment follows a shared responsibility model between the cloud provider, Beacon, and the client. This model leverages the capabilities and resources of each participant to deliver broader and more effective security coverage. Cloud infrastructure has been certified and is in use by major organizations around the world, including for data and workloads covered by stringent privacy and confidentiality regulations and top-secret classifications.



# Cloud Provider

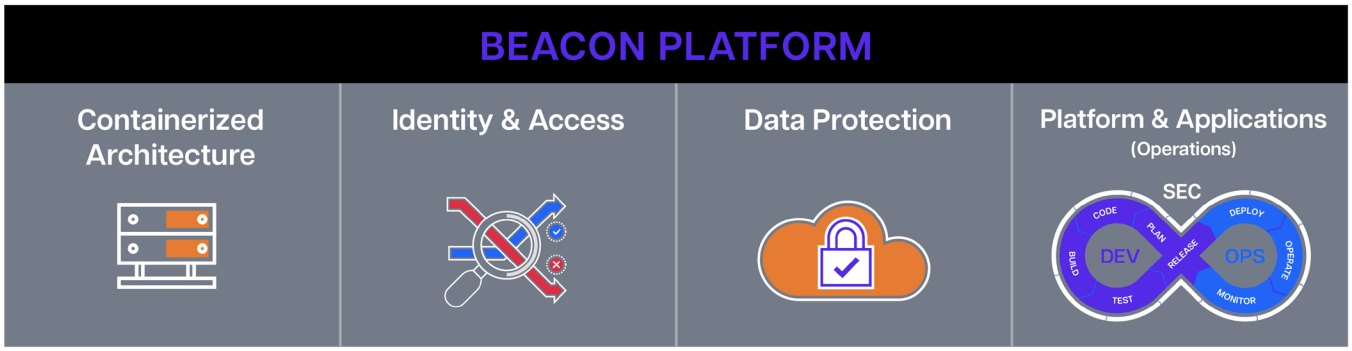



The cloud provider is responsible for security of the cloud infrastructure, including physical equipment and locations, identity and access controls, and the software that delivers the compute, storage, database, and networking functionality.

This includes:

- Physical and environmental security and access controls of cloud data centers and facilities.
- Identity services that securely manage and control access to cloud resources.
- Traffic inspection and filtering tools to prevent unauthorized access.
- Visibility and control of where data is stored and workloads are processed.
- Beacon services are deployed into cloud data centers chosen by the customer, which comply with national and regional data security laws and regulations. Major cloud providers offer services in multiple regions around the world.
- Privacy and confidentiality of data, including key management and automatic physical layer encryption of the cloud network, and additional encryption of data at rest and in transit implemented in Beacon Platform.
- Broad availability of third-party security technologies, enabling customers to layer on additional security products and services they already know and trust.
- Automation of many manual security tasks to reduce the risk of manual configuration errors and reduce response time to threats and alerts.
- Stringent security requirements for core infrastructure, including 24/7 monitoring by a large and experienced team of security experts, to help ensure confidentiality, integrity, and availability.
- Security audits and third-party validations are readily available to assess security functions, configurations, permissions, and other aspects of the cloud operating environment.

# Beacon Platform

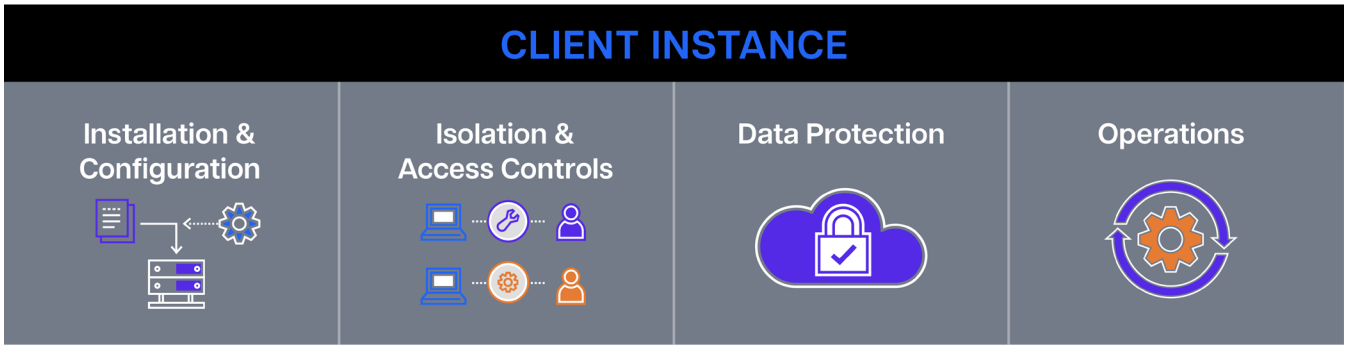



Beacon is responsible for the virtual machine images, code, containers, data encryption, and some configurations within the cloud infrastructure that each client uses in their individual, isolated Platform instances.

This includes:

- Security-by-design coding practices, automated governance, build, and test processes
- Hashes and digital signatures to securely identify and validate binary images and source code, from coding through customer operations.
- Logical segregation of development, testing, and production environments with role-based access controls.
- Customers choose when to pull updated, signed images into their specific instance, with ready fallback to earlier versions, if desired.
- Layered, containerized architecture, with each workload running in separate, isolated containers that communicate securely with each other over TLS.
- All containers and the control plane use the principle of least privilege, and none of them run with root authorization, limiting the potential attack surface.
- Automated container configuration templates and deployment for consistency and reduced risk of human errors are maintained through version control systems
- Standardized container, operating system, network, and firewall configurations, version controlled, and automatically maintained with all current security patches.
- Multi-package support to more easily add new capabilities without risking core functionalityEach workload runs with a minimally-acceptable package set, reducing operating risks, and enhancing overall stability.
- Encryption of data at rest and in transit with a minimum of 128-bit keys, private key generation and management by customers, and secure storage of keys and access tokens.
- Centralized monitoring, logging, and alerting tools that provide customers with detailed information on the status of their cloud instance, with immutable logs to prevent tampering.

# Client Instances




Each Beacon instance is installed directly into a customer's own cloud account or virtual private cloud. Security of each instance is delivered with a layered architecture that provides consistent installation, access controls, data protection, and automated processes. Clients are responsible for the security aspects of their individual and isolated instances, such as user roles and identities, data flow, and custom development, using a combination of Beacon components and existing corporate security processes and tools.

This includes:

- Fully automated installation based on version-controlled templates with multiple defense layers.
- Distinct workloads and data storage, accessible in cloud or client-hosted locations.
- Separate and isolated Beacon instance for each client, with firewalled perimeter that allows access via private
- IP address only when explicitly authorized and authenticated.
- Management of and authentication against corporate directory, single-sign-on tools, or preferred identity and access management systems.
- Full control over who, what, and when people have access, with role-based user accounts, multiple privilege levels, robust controls, and detailed access logs to meet the organization's policies, controls, and regulatory requirements.
- These can be connected to existing corporate identity and single-sign-on systems, including Active Directory or any other Security Assertion Markup Language (SAML) providers.
- Multi-factor authentication, digital certificates, and encryption across the Beacon Platform.
- Design and security of any data flows from Beacon Platform to client-hosted or external data sources, including data encryption at rest, in transit, and between workloads.

- Design and security of any data flows from Beacon Platform to client-hosted or external data sources, including data encryption at rest, in transit, and between workloads.
- Interfaces and integrations with a wide range of data sources which remain under the control of the client at all times. Beacon does not store client data in its own cloud instances.
- Secure key management infrastructure with unique keys for each client and full control and ownership of the key generation and management process.
- Automated build and refresh of workloads, ensuring that startup configurations, patching, and other maintenance is performed continuously, including rapid patching of vulnerabilities.
- Additional firewall, virus scanning, and other security technologies and processes, beyond those provided by Beacon and the cloud provider.
- Security of any additional code developed by the client, although this can take advantage of the secure software development life cycle workflows that are enabled and automated by Beacon's development tools.

For more information, download the white paper
Sharing Responsibility for Secure Cloud Operations.