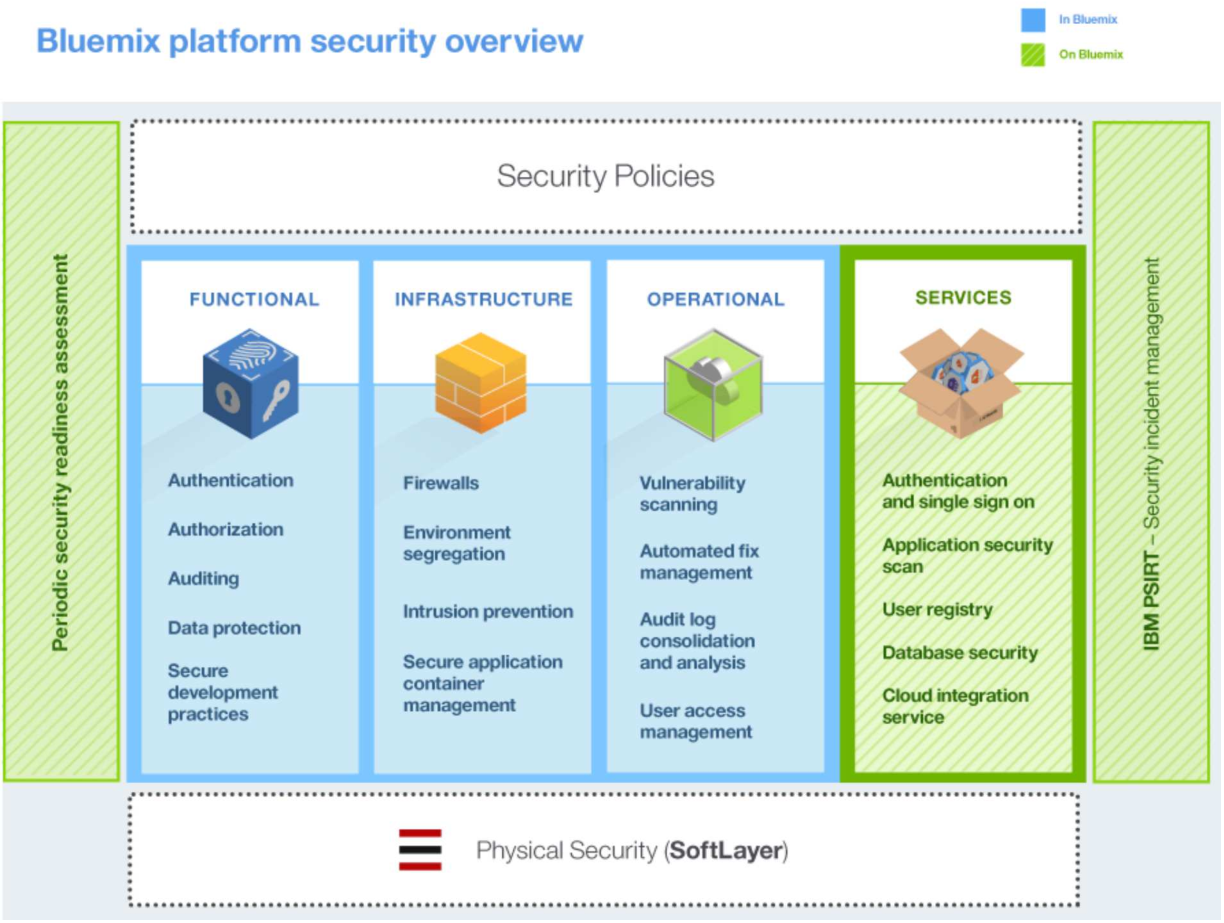
Security of the Bluemix platform

Bluemix provides functional, infrastructure, operational, and physical security (through IBM SoftLayer) for the core platform. However, Bluemix Local is unique in that the customer provides the infrastructure and data center, and owns the physical security.

The Bluemix environment on SoftLayer is compliant with the most restrictive IBM information technology (IT) security standards, which meet or exceed the industry standards. These standards include the following:

- Network, data encryption, and access control
- Application ACLs, permissions, and penetration testing
- Identification, authentication, and authorization
- Information and data protection
- Service integrity and availability
- Vulnerability and fix management
- Denial of service and systematic attacks detection
- Security incident response

Figure 1. Bluemix platform security overview



Bluemix platform security overview

🟦 In Bluemix
▨ On Bluemix

Periodic security readiness assessment

Security Policies

FUNCTIONAL

Authentication

Authorization

Auditing

Data protection

Secure development practices

INFRASTRUCTURE

Firewalls

Environment segregation

Intrusion prevention

Secure application container management

OPERATIONAL

Vulnerability scanning

Automated fix management

Audit log consolidation and analysis

User access management

SERVICES

Authentication and single sign on

Application security scan

User registry

Database security

Cloud integration service

IBM PSIRT – Security incident management

Physical Security (SoftLayer)

Functional security

Bluemix provides various functional security capabilities, including user authentication, access authorization, auditing of critical operations, and data protection.

Authentication

Application developers are authenticated toBluemix by using the IBM web identity.

For Bluemix Dedicated and Local, authentication through LDAP is supported by default. On request, authentication through IBM web identity can be set up instead for Bluemix.

Authorization

Bluemix uses Cloud Foundry mechanisms to ensure that each application developer has access only to the applications and service instances that they created. Authorization to Bluemix services is based on OAuth. Access to all Bluemix Platform internal endpoints are restricted to external users.

Auditing

Audit logs are created for all successful and unsuccessful authentication attempts of application developers. Audit logs are created also for privileged access to Linux systems that host the containers where Bluemix applications run.

Data protection

All Bluemix traffic goes through the IBM WebSphere® DataPower® SOA Appliances, which provide reverse proxy, SSL termination, and load balancing functions.
The following HTTP methods are allowed:

- DELETE
- GET
- HEAD
- OPTIONS
- POST
- PUT
- TRACE

HTTP inactivity times out at 2 minutes.

The following headers are populated by DataPower:

$wsis

Set to true if client-side connection is secure (HTTPS), set to false otherwise.

$wssc

Set to one of the following schemes of client connection: https, http, ws, or wss.

$wssn

Set to host name that is sent by client.

$wssp

Set to server port that client connects to.

x-client-ip

Set to client IP address.

x-forwarded-proto

Set to one of the following schemes of client connection: https, http, ws, or wss.

Secure development practices

For Bluemix Public and Dedicated, periodic security vulnerability scans are performed on various Bluemix components by using IBM Security AppScan® Dynamic Analyzer and static analyzer offerings. Threat modeling and penetration testing are performed to detect and address any potential vulnerabilities for all types ofBluemix deployments. In addition, application developers can use the AppScan Dynamic Analyzer service to secure their web apps that are deployed on Bluemix.

Infrastructure security

Bluemix builds upon Cloud Foundry to provide a robust foundation for running your applications. Within the architecture, several components are provided for security and isolation. In addition, change management and backup and recovery procedures are implemented to ensure integrity and availability.

Environment segregation

For Bluemix Public, development and production environments are segregated from each other to improve application stability and security.

Firewalls

Firewalls are in place to restrict access to the Bluemix network. For Bluemix Local, your company firewall segregates the rest of your network from your Bluemix instance.

Intrusion protection

Bluemix Public and Dedicated enable intrusion protection to discover threats so that they can be addressed. Intrusion protection policies are enabled on firewalls.

Secure application container management

Each Bluemix application is isolated and runs in its own container that has specific resource limits for processor, memory, and disk.

Operating system security hardening

IBM administrators perform network and operating system hardening regularly by using tools such as IBM Endpoint Manager.

Operational security

Bluemix provides a robust operational security environment with the following controls.

Vulnerability scan

Bluemix uses the Tenable Network Security vulnerability scanning tool, Nessus, to detect any issues with network and host configurations so that the issues can be resolved.

Automated fix management

Bluemix administrators ensure that fixes for operating systems are applied at appropriate frequencies. Automated fixes are enabled by using IBM Endpoint Manager.

Audit log consolidation and analysis

Bluemix uses the IBM Security QRadar® tools to consolidate Linux logs to monitor privileged access on Linux systems. Bluemix also uses IBM QRadar security information and event management (SIEM) to monitor successful and unsuccessful login attempts of application developers.

User access management

Within Bluemix, Separation of Duties guidelines are followed to assign granular access privileges to users, and to ensure that users have only the access that is required to perform their jobs according to the principle of least privilege.

Within a Bluemix dedicated or local environment, assigned administrators can manage roles and permissions for Bluemix user in their organization by using the Admin Console. See Managing your Dedicated instance with the Admin Console for details.

Physical security

Bluemix Public and Dedicated relies on the *network-within-a-network* topology of SoftLayer for physical network security. This network-within-a-network architecture ensures that systems are fully accessible only to authorized personnel. For Bluemix Local, you own the physical security for the local instance. Your data center is secured behind your company firewall.

In SoftLayer network-within-a-network, the *public network layer* handles public traffic to hosted websites or online resources. The *private network layer* allows for true out-of-band management through a distinct stand-alone third carrier over SSL, PPTP, or IPSec VPN gateways. The *data center to data center network layer*provides free and secure connectivity between servers that are housed in separate SoftLayer facilities.

Every SoftLayer data center is fully secured with controls that meet SSAE 16 and industry-recognized requirements, without exceptions. For more information, see the SoftLayer Security Compliance page.

Data security

With Bluemix, securing your data against unauthorized access is a joint effort between Bluemix and you.

Data that is associated with a running application can be in one of three states: data-in-transit, data-at-rest, and data-in-use.

Data-in-transit

Data that is being transferred between nodes on a network.

Data-at-rest

Data that is stored.

Data-in-use

Data that is not currently stored, and is being acted upon at an endpoint.

Each type of data needs to be considered when you plan for data security.

The Bluemix platform secures data-in-transit by securing the end-user access to the application by using SSL, through the network until the data reaches IBM DataPower Gateway at the boundary of the Bluemixinternal network. IBM DataPower Gateway acts as a reverse proxy and provides SSL termination.

Security for both data-in-use and data-at-rest is your responsibility as you develop your application. You can take advantage of several data-related services available in the Bluemix Catalog to help with these concerns.

Security of Bluemix applications

As an application developer, you must enable the security configurations, including application data protection, for your applications that run on Bluemix.

You can use security capabilities that are provided by several Bluemix services to secure your applications. AllBluemix services that are produced by IBM follow IBM secure engineering development practices.

SSO service

IBM Single Sign On for Bluemix is a policy-based authentication service that provides an easy to embed single sign-on capability for Node.js or Liberty for Java™ applications. To enable an application developer to embed single sign-on capability into an application, the administrator creates service instances and adds identity sources.

The Single Sign On service supports several identity sources where your users' credentials are stored:

SAML Enterprise

A user registry with an exchange of SAML tokens that completes the authentication.

Cloud Directory

A user registry that is hosted in IBM Cloud.

Social identity sources

The user registries that are maintained by Google, Facebook, and LinkedIn.

For more information, see Getting started with Single Sign On.

AppScan Mobile Analyzer

This service provides a security analysis of Android mobile applications. To use this service, you must upload a compiled Android app as an APK file. When the security analysis scan is done, you can download a report.

For more information, see Getting started with AppScan Mobile Analyzer.

AppScan Dynamic Analyzer

This service provides a security analysis of web applications with a dynamic analysis tool. The tool works on the deployed web app, not on the app source code, and it can scan any Bluemix web app regardless of its language or technology. You can scan only applications of the organizations that you belong to. To create a scan, you must configure the web app URL and the login credentials if any. When the scan is done, you can download a report.

For more information, see Getting started with AppScan Dynamic Analyzer.

Mobile Analyzer for iOS (Beta)

The Mobile Analyzer for iOS service provides AppScan dynamic security analysis for iOS mobile applications. It helps you identify security issues in your iOS mobile apps.

For more information, see Getting started with Mobile Analyzer for iOS.

Static Analyzer (Beta)

The Static Analyzer service enables static application security testing on the cloud. It helps you find source code vulnerabilities early in the software development lifecycle, so that they can be fixed before deployment.

Static Analyzer enables you to scan Java and Java web content by using a command-line interface (CLI) on your local disk. In addition, you can run a small installer that adds Static Analyzer plug-ins to Eclipse or Maven. You can use the client utility to scan and gather information about your files in an archive file that you then submit to the cloud for scan results.

For more information, see Getting started with IBM Static Analyzer for Bluemix.

IBM UrbanCode plug-in for application security testing

The IBM Application Security Testing for Bluemix plug-in enables you to run security scans on your web or Android apps that are hosted on Bluemix. This plug-in is developed and supported by the IBM UrbanCode™ Deploy Community on the IBM Bluemix DevOps Services platform.

For more information, go to IBM Application Security Testing for Bluemix.

SQL Database

The SQL Database service adds a fully provisioned relational database to your app. This service uses IBM Directory Server LDAP for authentication and IBM InfoSphere® Guardium® Data Activity Monitor to protect the database that is accessed by applications. The connection between applications and the database is protected by the SSL certificate that DigiCert signs.

In certain plans with this service, you can use the SQL database console in Bluemix to get reports that contain the following information:

- Sensitive data that might exist in the database that is accessed by applications.
- The application users who accessed the database within a specified period.
- The application users who are accessing sensitive data that is in the database.

To mask data by using SQL, applications can call the masking user-defined functions (UDFs) that are deployed together with the database. For example, you can mask the data that you want to use elsewhere for testing. The UDFs implement the data masking algorithms from IBM Infosphere Optim™.

The premium plan for this service also includes data encryption. For more information about this service, seeGetting started with SQL Database.

dashDB

The dashDB™ service uses IBM Directory Server LDAP for user authentication and IBM InfoSphere Guardium Data Activity Monitor to protect the database that is accessed by applications. The connection between applications and the database is protected by SSL certificates. This service uses the DB2® native encryption capability to automatically encrypt your deployed database and database backups. Master key rotation is automatic and happens every 90 days.

For more information, see Getting started with dashDB.

Cloud Integration

The Cloud Integration service enables you to integrate cloud and on-premises data. You can add a service to interact with backend databases such as DB2, Oracle, and SAP. Next, you can move data or create REST APIs for Bluemix applications to access and use. The service enables secure communication with on-premises secure connectors, and exposes backend systems of record as REST APIs to be used by applications.

For more information, see Getting started with Cloud Integration.

Secure Gateway

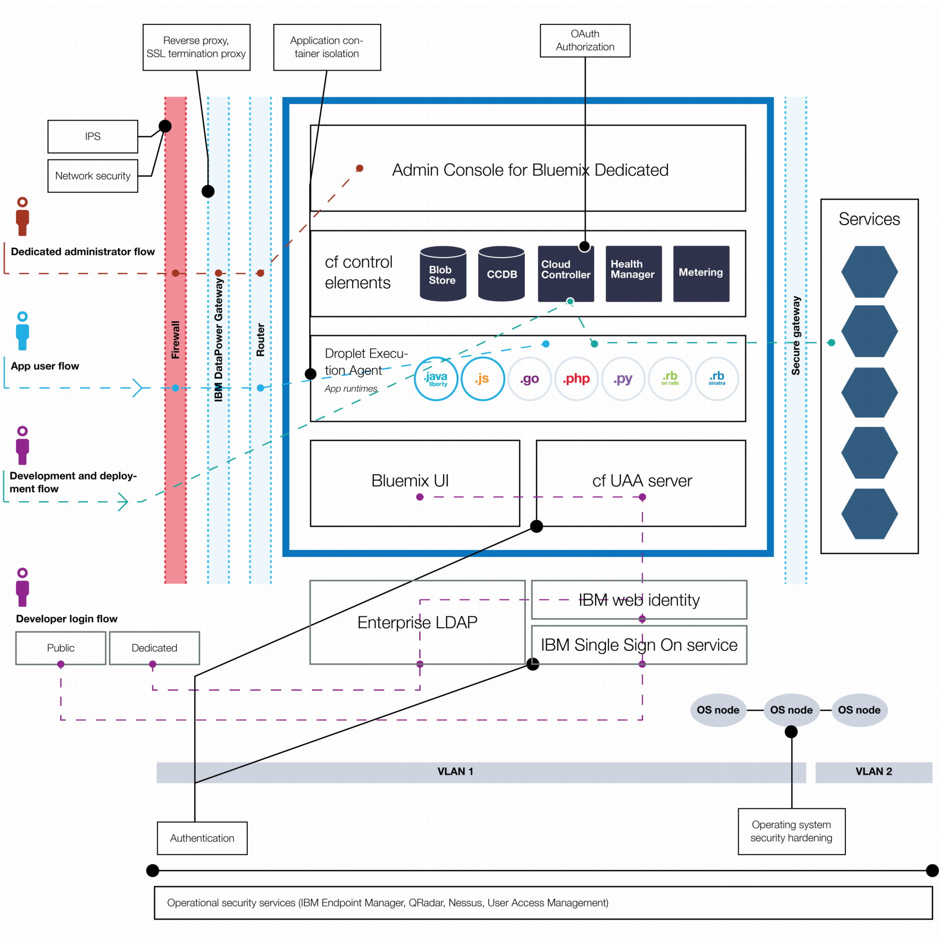
The Secure Gateway service enables you to securely connect Bluemix apps to remote locations, either on premises or in the cloud. It provides secure connectivity and establishes a tunnel between your Bluemixorganization and the remote location that you want to connect to. You can configure and create a secure gateway by using the Bluemix user interface or an API package.

For more information, see Getting started with Secure Gateway.

Bluemix security deployment

Bluemix security deployment architecture includes different information flows for app users and developers to ensure secure access.

Figure 2. Bluemix security deployment architecture



The information flow for Bluemix *app users* is as follows:

Through a firewall, with intrusion prevention and network security in place.

Through the IBM DataPower Gateway with reverse proxy and SSL termination proxy.

Through the network router.

Reaches the application runtime in the droplet execution agent (DEA).

The Bluemix *developer* follows two main flows, for login and for development and deployment.

- The developer flow for login includes the following:
    - For developers who are logging in toBluemix Public, the flow is as follows:

        Through the IBM Single Sign On service.

        Through IBM web identity.

    - For developers who are logging in toBluemix Dedicated or Local, the flow is through the enterprise LDAP.

- The developer flow for app development and deployment is as follows:

  Through a firewall, with intrusion prevention and network security in place.

  Through the IBM DataPower Gateway with reverse proxy and SSL termination proxy.

  Through the network router.

  Through authorization by using Cloud Foundry cloud controller, to ensure access to only apps and service instances that are created by the developer.

In addition to users described in these paths, an authorized IBM security operations team performs various operational security tasks, such as the following:

- Vulnerability scans. For Bluemix Local, you own physical security and any scans within your firewall.
- User access management.
- Operating system hardening by periodically applying fixes with IBM Endpoint Manager.
- Management of risks with intrusion protection.
- Security monitoring with QRadar.
- Security reports available through the Admin Console.