AWS Security Overview

BlueBin Tech

Table of Contents

Version History

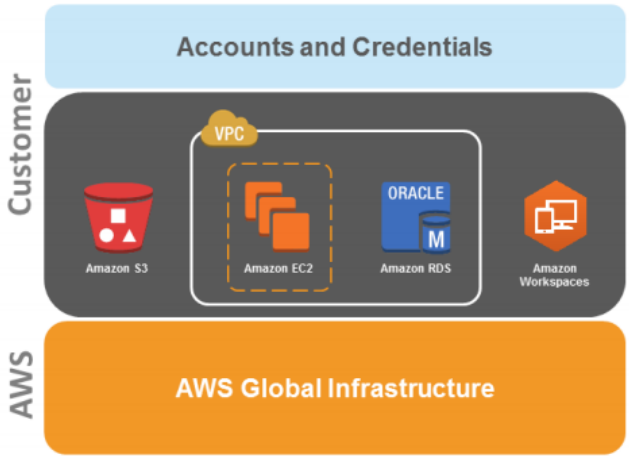
Version	Author	Date	Description
1.0	John Ratte	1/10/2015	First Version Complete.
2.0	Gerry Butler	10/1/2015	Updates inserted for hosted model
3.0	Gerry Butler	1/1/2016	Policy Review updates

Overview

Amazon Web Services (AWS) delivers a scalable cloud computing platform with high availability and dependability, providing the tools that enable customers to run a wide range of applications. Helping to protect the confidentiality, integrity, and availability of customers' systems and data is of the utmost importance to AWS, as is maintaining customer trust and confidence. BlueBin currently utilizes these services and infrastructure to host our Web Servers and Database Servers.

Shared Security Responsibility Model

Security in the cloud is slightly different than security in on-premises data centers. When moving computer systems and data to the cloud, security responsibilities become shared between you and your cloud service provider. In this case, AWS is responsible for securing the underlying infrastructure that supports the cloud, and BlueBin is responsible for anything put on the cloud or connected to the cloud. This shared security responsibility model reduces operational burden/costs improves the default security posture without additional action.



The amount of security configuration needed varies depending on which services are selected and how sensitive the hosted data is. Since BlueBin does not host any Protected Health Information (PHI), security needs are reduced. However, there are certain security features—such as individual user accounts and credentials, SSL/TLS for data transmissions, and user activity logging—that are still configured.

AWS Security Responsibilities

Amazon Web Services is responsible for protecting the global infrastructure that runs all of the services offered in the AWS cloud. This infrastructure is comprised of the hardware, software, networking, and facilities that run AWS services. Protecting this infrastructure is AWS's number one priority, and while you can't visit AWS data centers or offices to see this protection firsthand, AWS provides several reports from third-party auditors who have verified our compliance with a variety of computer security standards and regulations (for more information, visit (aws.amazon.com/compliance). Note that in addition to protecting this global infrastructure, AWS is responsible for the security configuration of its products that are considered managed services (such as Operating Systems). These services provide the scalability and flexibility of cloud-based resources with the additional benefit of being managed. For these services, AWS will handle basic security tasks like database patching, firewall configuration, and disaster recovery. For most of these managed

services, BlueBin has configured logical access controls for the resources and protect account credentials internally. A few of them may require additional tasks, such as setting up database user accounts, which is done by BlueBin for hosted SQL Server 2012 installations, but overall the security configuration work is performed by the service.

BlueBin Security Responsibilities

AWS products that fall into the well-understood category of Infrastructure as a Service (IaaS)—such as Amazon EC2, Amazon VPC, and Amazon S3—are under BlueBin control and require BlueBin to perform all of the necessary security configuration and management tasks. For example, for EC2 instances, BlueBin is responsible for management of the guest OS (including updates and security patches), application software or utilities you install on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance. Information on these is below. Individual AWS Account credentials are protected through individual user accounts with Amazon Identity and Access Management (IAM) so that each of our users have their own credentials with segregation of duties. Multi-factor authentication (MFA) is done with each account, through Access Control Lists (ACL) that are whitelist controlled for our AWS resources. API/user activity logging is done with AWS CloudTrail.

Web Servers

Operating System

Windows Server 2012

Patch Policy

In the event that a critical BlueBin Product Software Patch is required, BlueBin shall certify and install all patches within seven (7) days from the date that the patch is made available. This applies to critical patches only, including, but not limited to, security issues, incorrect operation of the Software that materially impacts the safe or correct operation of the Software, etc.

Firewalls

- Restricted Access Control Lists based on hospital and BlueBin ip listings
- VPC security groups restricting RDP access
- HTTPS access

Database Servers

Database Safeguards

In the BlueBin multi-tenant SaaS deployment, the data of multiple enterprises is located in separate data stores. Safeguards (described below) have been adopted to ensure that data of one tenant is not accessible to other tenants.

- In the multi-tenant SaaS environment, data will be segregated and isolated by separate Client databases.
- Data processed in the BlueBin solution utilizes unique data connections and SSIS packages.
- User data access will be authenticated based on user credentials mapped to that user's organization and will be verified on every transaction.
- Direct database access is not available to end users.

Patch Policy

In the event that a critical BlueBin Product Software Patch is required, BlueBin shall certify and install all patches within seven (7) days from the date that the patch is made available. This applies to critical patches only, including, but not

limited to, security issues, incorrect operation of the Software that materially impacts the safe or correct operation of the Software, etc.

Firewalls

- Restricted Access Control Lists to Web Servers and Client whitelisted ips
- VPC security groups restricting RDP access
- SQL Port redirection

FTP Servers

Operating System

Windows Server 2012

Access Requirements

SFTP Client with Certificate Authority (CA)

Product Security

Password/Login Functionality

Access to the BlueBin components is controlled by two separate logins that maintain identical parameters. It is not necessary for each user to have access to all components.

1) Access to the BlueBin Client Portal
2) Access to the BlueBin Intelligence Dashboard

Each method supports role-based access and allows users to access only the necessary operations to perform his/her job. Once authenticated, user permissions within the application are determined by the role assigned to the user.

Password Parameters

- Account Password Minimum Length = eight (8) Characters
- Contain Upper and lower case letters
- Contain a number OR non-alpha-numeric character
- Cannot contain:
  - User's login ID
  - Blanks

Authentication

All users required to access the application are loaded into SQL tables. Hashing is used to encrypt password information.

Application Logging and Auditing

BlueBin supports robust logging of security relevant events. Below is a list of the events that are logged within the application:

- User ID of user
- Successful login attempts
- Date/Time of event
- Type of event

Customers will need to request audit logs from BlueBin Support.

Development Security Practices

BlueBin adheres to a Software Development Life Cycle (SDLC) methodology. It follows commonly used best practices for designing, developing, and deploying with secure features. Every release containing architecturally significant change requires an architecture review and comparison of data integrity and performance versus pervious versions.