EFI IQ Cloud Platform Security White Paper

45218169

8 February 2021

Contents

Copyright information

Trademarks

The APPS logo, AutoCal, Auto-Count, Balance, Best, the Best logo, BESTColor, BioVu, BioWare, ColorPASS, Colorproof, ColorWise, Command WorkStation, CopyNet, Cretachrom, Cretaprint, the Cretaprint logo, Cretaprinter, Cretaroller, DockNet, MarketDirect StoreFront, DirectSmile, DocBuilder, DocBuilder Pro, DocStream, Dynamic Wedge, EDOX, EFI, the EFI logo, Electronics For Imaging, Entrac, EPCount, EPPhoto, EPRegister, EPStatus, Estimate, ExpressPay, Fabrivu, Fast-4, Fiery, the Fiery logo, Fiery Driven, the Fiery Driven logo, Fiery JobFlow, Fiery JobMaster, Fiery Link, Fiery Prints, the Fiery Prints logo, Fiery Spark, FreeForm, Hagen, Inktensity, Inkware, Jetrion, the Jetrion logo, LapNet, Logic, MiniNet, Monarch, MicroPress, OneFlow, Pace, PhotoXposure, PressVu, Printcafe, PrinterSite, PrintFlow, PrintMe, the PrintMe logo, PrintSmith, PrintSmith Site, Printstream, Print to Win, Prograph, PSI, PSI Flexo, Radius, Rastek, the Rastek logo, Remoteproof, RIPChips, RIP-While-Print, Screenproof, SendMe, Sincrolor, Splash, Spot-On, TrackNet, UltraPress, UltraTex, UltraVu, UV Series 50, VisualCal, VUTEk, the VUTEk logo, and WebTools are trademarks of Electronics For Imaging, Inc. and/or its wholly owned subsidiaries in the U.S. and/or certain other countries.

All other terms and product names may be trademarks or registered trademarks of their respective owners, and are hereby acknowledged.

About This Document

This document provides details about how security technology and features are implemented within the EFI IQ cloud applications and platform. This document also discusses how the overall EFI IQ system design provides the groundwork for a secure cloud system environment in which end users, customers, the EFI team, and EFI's provider, Amazon Web Services (AWS), play important roles.

The included topics are user access and account control, hosting platform, EFI management of the hosted account, ongoing software maintenance, and threat mitigation. In addition, this document covers data collection and management including data privacy controls. The intent of the document is to help our customers combine EFI IQ security technology with their own policies to meet their specific security and data privacy requirements.

Disclaimer: Fiery products are designed to be used in production and office printing environments. Issues of GDPR compliance regarding data sent to, processed by, or stored on the Fiery digital front end or on an internal network are the responsibility of the printing system owner.

Overview of EFI IQ

EFI IQ is a cloud platform that includes a range of web applications for print service providers. Web applications on the EFI IQ cloud platform can improve print operations and print output quality. You can reduce downtime and maximize productivity by monitoring your print devices. EFI IQ provides print production analytics so you can make smarter and more informed decisions.

EFI IQ includes the following cloud applications[1]:

- EFI Cloud Connector (ECC)

  Connect print devices to EFI IQ.

- EFI ColorGuard

  Achieve consistent, accurate color quality on your Fiery Driven devices with a streamlined color verification process.

- EFI Manage

  Manage your printers by syncing resources, checking compliance, and monitoring device status.

- EFI Go

  Check printer status, review submitted jobs, and view history from your mobile device.

- EFI Insight

  Maximize utilization and profit from your print devices with accurate production tracking.

- EFI Notify

  Subscribe to scheduled production reports and alerts of production blocking events.

New functionalities and applications are added regularly to EFI IQ.

[1] Not all applications are available on all types of printers. Please refer to https://www.efi.com/products/efi-iq/.

Technology Platform Overview

EFI IQ web applications are built on modern technology platforms and make extensive use of current software industry best practices.

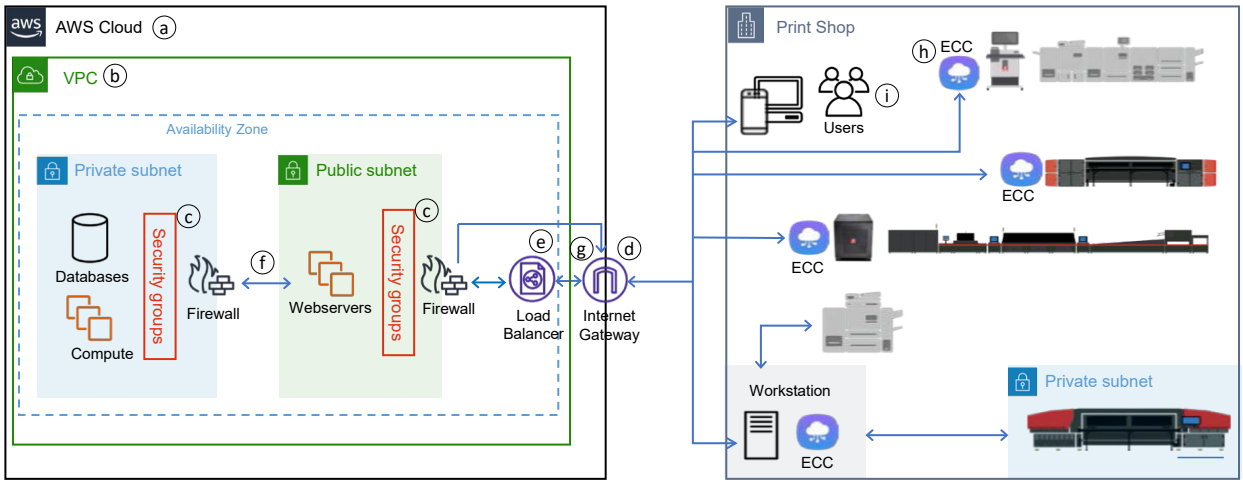
The EFI IQ system comprises two components: a collection of hardware and software which reside in the cloud, and the software and web applications on or near the devices being monitored. The devices monitored are typically printers, but are often referred to in the context of the cloud as "Internet of Things" (IoT) devices. IoT devices require a piece of software installed on or near them to connect securely to the cloud. In the EFI ecosystem, this software is the EFI Cloud Connector (ECC).

The cloud portion of EFI IQ is hosted on Amazon Web Services (AWS). The EFI IQ cloud is a collection of compute instances from the Amazon Elastic Compute Cloud (EC2). EFI has configured these inside of an Amazon Virtual Private Cloud (VPC). This architecture offers a secure public network to customers and their IoT devices while making it possible to segregate customer data within a secure private network that cannot be accessed by unauthorized users.

EFI deploys EC2 instances and installs standard AWS Ubuntu images. Once provisioned, EFI deploys its software microservices within Docker containers. EFI has chosen to use Docker containers because they offer a controlled, fault-tolerant environment in which to run its software. To facilitate deployment, EFI leverages the AWS Layers strategy which allows us to define a set of microservice containers that are deployed together. The use of layers facilitates horizontal scaling of the EFI IQ cloud. It is possible to deploy additional compute resources as overall load on the system grows.

All access is controlled by secure user credentials. Each account owner (EFI IQ customer) must create a User name based on a valid email address and is required to use a secure password.

Figure 1: Overview diagram of EFI IQ Cloud Platform



Callout	Explanation
a	EFI IQ Cloud is hosted on Amazon Web Services (AWS).
b	EFI has clusters of compute instances and databases that are organized in a Virtual Private Cloud (VPC). EFI segregates instances and data from unauthorized access from outside of the network. EFI's VPC uses Network Access Control Lists (NACLs) as a firewall for controlling network traffic.
c	Security groups provide an additional layer of defense at the instance level.
d	All network traffic uses https and WSS (WebSocket Secure) over port 443. The NACL rejects all requests that are not made on port 443.
e	The Elastic Load Balancer (ELB) is an AWS service that routes calls from the Internet to one of EFI's public facing elements (in the public subnet). Its intent is to balance the load among the available servers, to ensure high availability in case of failure, and to allow for upgrades without taking the system offline.
f	Once requests have been accepted via the VPC's public subnet, they are routed to the systems within the private subnet.
g	Data going back to the IoT devices or the web browsers are again routed through the public facing portion of the VPC over port 443.
h	In the customer site, the EFI Cloud Connector (ECC) is used to securely connect the printers (IoT devices) to the EFI IQ cloud. The ECCs can be installed on the Fiery digital front end (DFE), on the printer itself, or on a workstation with Internet connection in the print shop network.
i	Users in the print shop location (administrator and operator) can use EFI IQ applications to make better data-driven decisions.

Data collection

It is necessary to install the EFI Cloud Connector (ECC) on the device to control communication from the device to the EFI IQ cloud platform. The ECC initiates all communication to the EFI IQ cloud via WSS (WebSocket Secure) over port 443 and subsequent communication on that connection is bidirectional. If the printer or Fiery server is not directly connected to the Internet, it can connect to the EFI IQ cloud through an ECC instance that is set up on a workstation with Internet access. If at any point the ECC loses Internet connectivity, the ECC will cache data and resend it once connectivity is re-established.

Network security

EFI IQ uses an Amazon Virtual Private Cloud (VPC), which provides dedicated network ranges for EFI IQ within the AWS cloud. The EFI IQ system uses one VPC with one private and one public subnet. Network Access Control Lists (NACLs) on the VPC isolate and block access to service components that do not require Internet access.

Users of EFI IQ applications access web servers via the public facing subnet of the VPC. Only credentialed access is permitted. Once through this gate, there is only application-mediated movement of data to and from the private subnet. Data is returned to the users through the gateway.

This segregation helps protect private resources from attack by preventing unauthorized access.

The VPC structure also isolates the Production cloud from Test and Development clouds. Each of these clouds reside in their own VPC.

Firewalls

All of the cloud systems are protected by firewalls. The EFI IQ cloud opens port 443 for ECC and web application access. All other ports are closed. Within the VPC, EFI IQ uses named ports to communicate within micro-services. All instances in the VPC use network ACL and Security groups to control access and traffic.

As mentioned in Access control to cloud compute instances in EC2 on page 16, access to individual instances of the IQ cloud cluster is controlled by an allowed list of IP addresses. For example, a computer connected via the EFI corporate domain can attempt to access an instance of s cloud cluster via SSH (secure shell). All other computers outside the EFI corporate domain are denied SSH access.

Beyond firewall protection, access to the EC2 instances is strictly controlled using public key access. This is described in Access control to cloud compute instances in EC2 on page 16.

User Access and Control of EFI IQ Account

Definitions

This section defines how EFI IQ uses the terms Tenant, User, Group, and Company in this document.

- A Company, or customer, is the entity using one or more of the EFI IQ applications.
- A Tenant account is created for each company that utilizes the EFI IQ cloud.

  When creating a Tenant account, it is necessary to specify a company name, physical address, and at least one User.
- A User is an object within a Tenant and is used to log in to EFI IQ using a unique login name with a user role attribute. Additional User accounts can be created at the Tenant administrator's discretion. A User is an individual person with a unique login to the Company's Tenant account.

  Typical User attributes include: first and last name, Company (the Tenant account the User belongs to), user role, and assigned devices via individual devices or the device collections.

  User account passwords must be 8 or more characters long with at least:

  - One lowercase letter
  - One uppercase letter
  - One number
  - One symbol

  If a user fails to correctly enter a password four consecutive times, the user will be invited to reset the password. If, however, the user chooses not to reset the password, the account will remain locked for 10 minutes. Any attempt to enter a password during that 10 minute period will be refused and the 10 minute waiting period will be restarted.
- An EFI IQ admin user is a User with admin role within the EFI IQ account. EFI IQ admin users manage objects such as User, Group, Devices, Company, etc. EFI IQ admin users can grant admin rights to other users within the account.
- A Group is an object used to grant Users access to printers in a Tenant.

  EFI IQ admin users can assign Users with Group(s) so that only specified Users can access specific devices.

User access to data

All Users of EFI IQ applications are required to have User IDs and passwords. User IDs must be valid email addresses which may or may not be Personally Identifiable Information (PII). When establishing an EFI IQ account, account creation is guarded by Captcha to minimize the risk of automated malicious account creation and access.

Users are authenticated into a company's Tenant account. Within the EFI IQ applications, the admin can invite other Users from their organization to see some or all data from the devices or a subset of devices, based on their role in the customer's organization.

When a User first signs up for EFI IQ, a new Tenant account is created for the User. For example, if Bob Jones of Company ABC creates a Tenant account with an email address of bob.jones@company-abc.com, then that e-mail address acts as his username. When Bob invites Nancy Smith to become a User in his Tenant account, her User name is nancy.smith@company-abc.com. Nancy is a User in the Company ABC Tenant account and can be assigned access to some or all of the data in the Tenant account. Users of other Tenant accounts have no access to data in Company ABC Tenant.

Data segregation

As a multi-tenant application, EFI IQ requires a valid user token in order for a user to access the Tenant data. Users from one Tenant have no access to data from another Tenant account. The administrator can specifically invite users from outside their Tenant account to join their account with specific privileges. For example, Company ABC may want to invite a reseller service representative to see certain data or printer status.

Management of User rights, privileges, and/or entitlements

A User profile contains information about the User and the User's status. Profile information includes the User's role in the company such as administrator or operator. An administrator has access to all printers and all features of licensed EFI IQ applications. Non-administrator roles, such as an operator role, do not have access to the admin features and must be explicitly granted access before viewing, for example, a printer's production data. Operators can be assigned access to data about specific printers. The administrator can easily assign one or more printers to a Group of Users. If a User with an operator role is added to a Group, the operator will be granted access to the printers in that Group and only the printers in that Group.

Session management

EFI IQ web applications use AWS Cognito and a combination of JSON Web Tokens (JWT) and Web Storage for session management. Passwords entered when signing in are passed directly to Cognito and are not stored or used anywhere in EFI IQ. All session management authorization is handled solely with the access and refresh tokens provided by Cognito.

The Access Token uses the industry-standard JWT or JSON web token (RFC 7519) method for representing claims securely between two parties. This token is usable only in secure contexts (HTTPS) and is a short-lived token (1 hour) used for server-side REST API validation. Once the Access Token expires or becomes invalid, the client makes use of the Refresh Token to get a new Access Token and extend the client session.

The Refresh Token is a secure token with no way to decrypt it at the client-side. The life of the Refresh Token is configurable in AWS Cognito, which we have set to 7 days. If the user logs out from EFI IQ app manually, both the Access Token and Refresh Token are invalidated.

The access and refresh tokens are stored in Local Web Storage in the browser. Local Web Storage is protected from access by unrelated domains by the Same Origin Policy. The Same Origin Policy restricts how a script or page loaded from one domain can interact with resources from another domain and helps isolate potentially malicious pages, reducing attack vectors.

Data export

The EFI IQ user who has access to an application can export production data of the devices assigned to that user from the Tenant account in a comma-separated values (CSV) file format. The user can also use an EFI IQ cloud API to export data to be used in another business system. The decision to export is in the user's control and the resultant file is delivered to the user. To perform these downloads, the user must have entered a valid username/password combination to access the Tenant account. File downloads are always performed using secure session tokens as part of their browser session.

Users can subscribe to daily, weekly, or monthly production summaries from the devices assigned to that user, which are emailed to them. As with file exports, the reports are controlled by the users and emailed only to their verified email addresses.

Hosting of EFI IQ

EFI IQ cloud platform is hosted on Amazon Web Services (AWS) in Ireland. EFI IQ is currently not available as a private hosted on-premises application. User data is stored at AWS location in EU-West-1 region.

AWS physical security

Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Please refer to AWS documentation (https://aws.amazon.com/compliance/data-center/controls/ or https://aws.amazon.com/security/) for physical security at AWS hosting sites regarding:

- Access permissions, including two-factor authentication a minimum of two times to access data center floors
- Video surveillance, monitoring, retention policy, etc.
- Visitor or guest policies, including escorts
- Security of site

AWS environmental controls

Per AWS documentation https://d1.awsstatic.com/whitepapers/aws-security-whitepaper.pdf, the hosting location(s) have:

- Fully redundant power systems fed via different grids from independent utilities to further reduce single points of failure
- Uninterruptible Power Supply (UPS) units that provide back-up power in the event of an electrical failure
- Generators to provide back-up power for the entire facility
- Climate control to maintain a constant operating temperature for servers and other hardware
- Fire detection and suppression systems
- Leakage detection systems

AWS data center locations are carefully selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity.

AWS certifications

AWS certifications are listed at https://aws.amazon.com/compliance/programs/.

Hardware maintenance

AWS monitors electrical, mechanical, and support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

System availability

Availability, or "uptime," for EFI IQ cloud customers has exceeded 99.8%, excluding announced events for maintenance.

EFI has two categories of system downtime: planned and unplanned. By design, many maintenance operations can be performed with no interruption to service. Every effort is taken from development though delivery to ensure any necessary planned outages are brief and infrequent.

Various components are monitored around the clock from points around the world. Problems often are detected, isolated, and resolved without customer impact. The actions provide an early warning system that permits the team to proactively prevent problems.

Data hosting and backup sites

EFI hosts its cloud in a single AWS Region. Data is automatically backed up to one or more Availability Zones (AZ) within that region.

In the event of a severe AWS outage of the AZ, where the EFI IQ cloud is deployed, EFI can manually redeploy the cluster of servers in another AZ and redeploy with backed up data.

Once a new cluster in another site is established, the ECCs installed on IoT devices will send the cached production data to the new cluster.

Disaster recovery and business continuity

In the unlikely event that user data is lost or damaged, EFI maintains full data backups within the AWS infrastructure and has processes for restoring the lost data. EFI employees in the US and India can manage EFI IQ applications should there be a business disruption in one location.

AWS audit rights

EFI relies on Amazon Web Services which maintains and publishes numerous third-party audits and certifications (see https://aws.amazon.com/compliance/programs/). There is no right to directly audit AWS. Amazon's Internal Audit group reviews the AWS services resiliency plans, which are also periodically reviewed by members of the Senior Executive management team and the Audit Committee of the Board of Directors.

EFI Management of AWS Account

EFI access to AWS account

Access to AWS is securely controlled. EFI uses Amazon Identity and Access Management (IAM) so that each user has their own credentials and EFI can implement segregation of duties. IAM groups for admins and non-admins are used for managing access to AWS resources. EFI has IAM roles in place to control IQ access to other AWS services. EFI makes use of IAM policies for access privilege delegation.

Access to AWS by EFI engineers requires multi-factor authentication (MFA). Access occurs via secure web browser session (HTTPS), and is logged. AWS/IAM passwords require a minimum password length of 14 characters and reuse of passwords is prohibited.

- MFA by a physical token or mobile app is required for all accounts.
- Strict IAM roles are assigned to all EFI employees with access to AWS.
- EFI limits the commands (on a role basis) that can be executed on a particular system.

Access control to cloud compute instances in EC2

EFI IQ is hosted on Ubuntu Linux servers. EFI IQ uses SSH version 2 with non-root privileged accounts to manage Linux servers hosted in AWS. Only a limited number of EFI employees have access to AWS accounts and even fewer have access to compute instances in EC2.

EFI employees accessing AWS cloud compute instances must use EFI-supplied computers with standard hardware and software that are compliant to EFI security policy. They also must follow EFI's security practices.

All system access to individual compute instances by EFI employees is controlled through public/private key pairs. There are no passwords to hack/crack. Those EFI employees with access have their public keys stored on the compute instances. All others will fail.

EFI allows access only from the following specific locations:

- The EFI domain

  A list of public IP addresses for those individuals who need access.
- The list of public IP addresses is maintained on a "need-to-access" basis.

Role related permissions

Permission to access data stored on AWS is restricted to just a few EFI employees and it is granted only when needed to investigate a specific problem reported by a customer.

EFI reserves the right (as described in EFI end user license agreement) to collect anonymized information about the data in the system and user interaction with web applications. No PII is gathered and the data gathered is aggregated with all other data from the system.

Management of security incidents

If a security or abuse incident should occur, AWS has an EFI contact available 24/7 to respond to a case. If a resource or instance is compromised, EFI will take immediate action.

EFI uses the AWS Abuse reporting process to resolve any issues, originally detected by either EFI or AWS. Upon discovery of a compromised or infected Amazon EC2 instance or AWS resource, EFI redeploys the affected services.

Data Collection and Management

Print production data collected

EFI IQ stores print production data such as job log information, job submission mode, color measurement data, digital printer and server model, server configuration and status, and configuration and operational status information from the IoT device. The content of a print job is not sent to the cloud. The print job name and a thumbnail of the first page are sent to the cloud unless disabled by the user.

User data collected

Personal data for a company's employees who join the company's IQ Tenant account consists of first name, last name, email address, and phone number. EFI IQ account creation requires company name and physical address information. Customers can also specify additional information for all operational locations they wish to individually track.

EFI use of Personally Identifiable Data

EFI will use Personally Identifiable Data for the following purposes:

- Maintain the customer account
- Authenticate users
- Complete commercial transactions such as fulfill purchase orders for licenses
- Communicate license status, production alerts, scheduled notifications, and product changes
- Provide usage of the EFI IQ applications
- Send print production reports and alerts as requested by user
- Provide technical support
- Close accounts

Data location

Currently, the data is housed in the EU-West-1 Region of AWS. All hosted systems and customer data reside in secure AWS facilities within this Region.

Certain information about an account and user may be transferred to systems in the US for the purposes of customer service (order entry, acknowledgement, invoicing, etc.), technical support, and customer communication.

Transfer of data from the European Union

EFI IQ applications involve very few data elements that are classified as PII under General Data Protection Regulation, or GDPR (see User data collected on page 18). EFI relies on Standard Contractual Clauses (SCCs), per the European Commission, that govern import and export of data between EFI group companies. When signing up for an EFI IQ account, the customer chooses whether to accept the safeguards in the SCC.

EFI processing activities include:

- Establishing and maintaining a customer account including User authentication
- Fulfilling a purchase order and delivering customer service
- Sending email or text communications to a mobile phone to deliver alerts, notifications, status, reports, and product change information
- Inviting additional Users to an account via email when directed by the account administrator
- Deactivating licenses and rehosting them from one printer to another printer
- Providing technical support
- Deleting data upon request
- Closing accounts

Data in transit security

All EFI IQ applications implement TLS encryption for security-sensitive traffic, such as pages dealing with login and password information.

EFI IQ uses Secure WebSocket (wss) for our ECC to cloud data transfer.

All EFI IQ web applications, EFI Go, and EFI ColorGuard desktop application use https access and user authenticated sessions with security tokens for all access.

Data backup and destruction policy

- Print production data

  The databases for print production data are backed up as a rolling backup. Backups occur hourly each day with a final backup made for each day. There are backups for 6 days that roll into a weekly backup. The four most recent weekly backups are retained. For example, it is possible to restore a snapshot of data from 25 days ago, but not of 40 days ago. Each backup contains data for each Tenant account, which can extend for a maximum of 3 years.

  Backups do not extend past 28 days in order to meet the GDPR requirement that user data must not be retained in any form for longer than 30 days after a customer requests that their data be removed from the system.

- Account data

  The EFI IQ databases containing Tenant, User, and printer static data are protected through redundancy and automatic snapshots. There is a main server and a standby server. The standby server is always a duplicate of the main server. The two servers are in separate Availability Zones within the AWS Region. If the main server goes down, the standby server is engaged for seamless processing of user requests. In addition to this, snapshots of the data are taken every 5 minutes so data can be restored if necessary.

EFI access to data

EFI employees have access to data in the cloud only through AWS's IAM. Individual access is limited based on need-to-use and skill level under the direction of EFI's Director of Cloud Engineering. EFI employees are required to pass appropriate background checks and are required to sign confidentiality agreements. Ongoing training of operations personnel in the matters of security and privacy occurs regularly.

All rights within an application and infrastructure are granted on a per-user basis, with group-based assignments possible. For example, a customer service group may be granted the right to change (or request a change) for a given user or customer to fulfill a purchase order for a subscription to an EFI IQ application. Access to user account username for technical support or customer service personnel is allowed only in cases where it is reasonably required to assist customers. Such access is almost exclusively a limited, read-only view with no system control. System and database access are allowed only on a per-user basis for engineering personnel.

Data breach reporting

EFI has a written policy for the reporting of, and actions to be taken in response to, a confirmed EFI data breach involving PII. This policy is compliant with the State of California notification requirements and GDPR notification requirements.

EFI has not had a security breach of its EFI IQ application in the past. In the event of a data breach where outside assistance is required, EFI has a contract and NDA in place with FireEye.

Security Maintenance and Threat Mitigation

Software development process and quality assurance

Code changes are peer reviewed and then pass quality assurance testing prior to deployment. Once a new deployment occurs, tests are run on ongoing basis to ensure the applications are working as expected.

EFI employs procedures for reviewing and resolving reported issues. Problems may be reported by site monitoring, EFI quality assurance, customers, or other sources. Issues are triaged and resolved.

The EFI development process follows secure software development best practices, which include design reviews, threat modeling, and completion of a risk assessment.

Production, test, and development system environments are segregated. No common data, servers, network, or any other resource are shared by each environment.

EFI provides EFI IQ users with product documentation and training in the form of Help documentation, eLearning courses, and product information on www.efi.com.

Security updates

The AWS instance will be updated if there is a major security update to the OS image.

EFI updates and tests its software for security vulnerabilities (see Other security measures on page 22) and updates the software as appropriate.

Anti-virus software

The customer is responsible for running anti-virus software on the machines where they run the applications and Fiery server. EFI provides anti-virus software for machines used by EFI employees.

EFI IQ applications are hosted on Ubuntu Linux instances. In addition, our systems have limited access (as explained in Access control to cloud compute instances in EC2 on page 16) and thus are less susceptible to viral attack.

No emails are received by EFI IQ, so no email filtering or anti-spam capability is required.

In addition, EFI has implemented a security update management process that covers all AWS hosted instances to reduce the exposure to automatic spreading of malware. This is controlled by Chef, an infrastructure and app delivery tool. EFI explicitly specifies the packages that are installed on the system.

Software updates

For security updates, EFI always deploys previously created and tested Docker containers. These are standalone modules that are installed and executed. These closed systems cannot be altered without valid access to their storage or the systems to which they are deployed. EFI restricts access to systems which house Docker containers and the EC2 instances on which they are installed. EFI restricts permission to installing software to authorized EFI employees only.

The installation of these containers is controlled by a well-defined process, managed by a standard computer program called Chef. Valid and tested Docker containers are uploaded securely to AWS and then deployed using Chef. The use of Chef serves to document the deployment process and make it reproducible. Chef allows granular control so that when there are multiple versions of a particular container, only the specific, desired version is actually deployed. This makes redeployment reliable and safe, ensuring that the correct version is always redeployed. Chef also allows for automated roll back to a previous known-working configuration if problems are encountered with a new deployment.

Logging and monitoring

Previously in this document, we have discussed that EFI permits access to the individual compute instances that make up the EFI IQ cloud only through a allowed list of permitted IP addresses. This approach helps EFI protect the cloud from malicious intrusion.

EFI uses AWS CloudWatch to proactively monitor activity within the system. EFI uses it to monitor CPU and disk usage, memory usage, whether internal queues are backing up, and other system status indicators. These serve as early warning alarms to alert EFI to potential problems before they impact system performance or operation. Team members get email alerts and they work to diagnose and correct the root cause of the problem.

EFI makes extensive use of system logging. All the microservices have their own logs that are maintained for 30 days. EFI uses these logs to both forensically diagnose issues and to proactively decide when it is safe to retire deprecated interfaces. No customer identifiable information is stored in these logs and they are only examined by trained developers researching specific issues.

The software elements in the EFI IQ cloud have their own logging mechanisms. For instance, the web server logs all attempts to access the cloud. These logs record the API calls and the status code for each call so EFI can detect a variety of conditions from this data, including unauthorized attempts to access the cloud. In the past, EFI has used these logs to identify the source of malicious attacks and acted to turn off those IP addresses at the AWS Elastic Load Balancer level.

EFI uses AWS CloudTrail to record user API access to the system. EFI logs the endpoint requests, their status (but not the data returned), and the origin of the request.

Other security measures

EFI runs a BURP scanning report for EFI IQ applications prior to web release. Also, EFI releases the EFI IQ applications to third-party vulnerability scanners, such as Acunetix, to look for any vulnerabilities before releasing new application updates. The purpose of this is to proactively identify obsolete Javascript libraries and obsolete security methods in use.

The EFI IQ cloud relies on AWS infrastructure services to alert EFI to denial of service (DoS) attacks. EFI moves promptly to stem those attacks if they occur.