efi Productivity Suite

EFI Hosting Security White Paper
Version 3.0

EFI Productivity Suite | *EFI Hosting Security White Paper*

December 2019

Document Version 3.0

Patents

This product may be covered by one or more of the following U.S. Patents: 4,716,978, 4,828,056, 4,917,488, 4,941,038, 5,109,241, 5,170,182, 5,212,546, 5,260,878, 5,276,490, 5,278,599, 5,335,040, 5,343,311, 5,398,107, 5,424,754, 5,442,429, 5,459,560, 5,467,446, 5,506,946, 5,517,334, 5,537,516, 5,543,940, 5,553,200, 5,563,689, 5,565,960, 5,583,623, 5,596,416, 5,615,314, 5,619,624, 5,625,712, 5,640,228, 5,666,436, 5,745,657, 5,760,913, 5,799,232, 5,818,645, 5,835,788, 5,859,711, 5,867,179, 5,940,186, 5,959,867, 5,970,174, 5,982,937, 5,995,724, 6,002,795, 6,025,922, 6,035,103, 6,041,200, 6,065,041, 6,112,665, 6,116,707, 6,122,407, 6,134,018, 6,141,120, 6,166,821, 6,173,286, 6,185,335, 6,201,614, 6,215,562, 6,219,155, 6,219,659, 6,222,641, 6,224,048, 6,225,974, 6,226,419, 6,238,105, 6,239,895, 6,256,108, 6,269,190, 6,271,937, 6,278,901, 6,279,009, 6,289,122, 6,292,270, 6,299,063, 6,310,697, 6,321,133, 6,327,047, 6,327,050, 6,327,052, 6,330,071, 6,330,363, 6,331,899, 6,340,975, 6,341,017, 6,341,018, 6,341,307, 6,347,256, 6,348,978, 6,356,359, 6,366,918, 6,369,895, 6,381,036, 6,400,443, 6,429,949, 6,449,393, 6,476,927, 6,490,696, 6,501,565, 6,519,053, 6,539,323, 6,543,871, 6,546,364, 6,549,294, 6,549,300, 6,550,991, 6,552,815, 6,559,958, 6,572,293, 6,590,676, 6,606,165, 6,633,396, 6,636,326, 6,643,317, 6,647,149, 6,657,741, 6,662,199, 6,678,068, 6,707,563, 6,741,262, 6,748,471, 6,753,845, 6,757,436, 6,757,440, 6,778,700, 6,781,596, 6,816,276, 6,825,943, 6,832,865, 6,836,342, RE33,973, RE36,947, D341,131, D406,117, D416,550, D417,864, D419,185, D426,206, D439,851, D444,793.

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.

Table of Contents

About This Document

This white paper provides current and prospective customers of EFI cloud applications with an overview of the security issues pertinent to the deployment and maintenance of a cloud-based system.

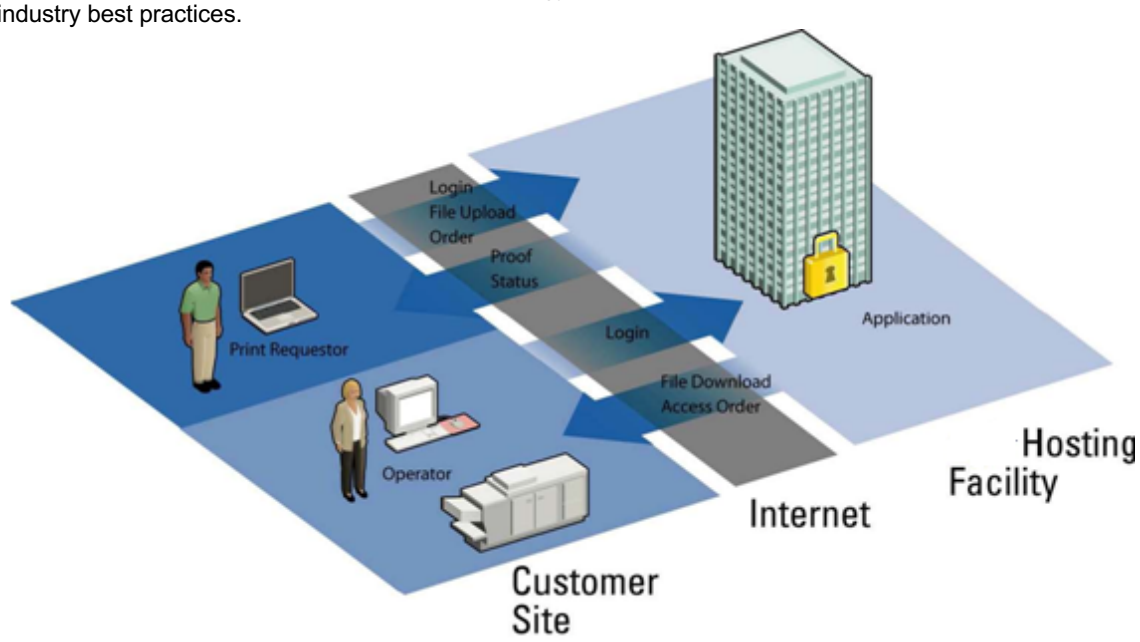
Introduction

EFI develops enterprise software for the printing industry. This software includes advanced Web applications that are in the cloud – hosted for you by EFI and delivered to you over the Internet. They are designed with security, availability, and performance in mind. The result is a secure means of doing business via e-commerce and e-production with your customers using standard Web browsers. The benefits of using a cloud application include avoiding the expense of on-site hardware and being assured of real-time maintenance at the hosting facility.

This white paper provides current and prospective customers of EFI cloud applications with an overview of the security issues pertinent to the deployment and maintenance of a cloud-based system

Technology Platform Overview

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



EFI Cloud Services routinely provides input to the application design process with performance, scalability, and security in mind. The following are common software design elements of EFI cloud applications.

Secure Communication

For the exchange of sensitive information, the system uses secure sockets (HTTPS, TLS) with the current strongest level of encryption available. Examples of sensitive information include logins, passwords, and credit card numbers or other payment information. Otherwise, the system uses normal HTTP. Some applications can be configured to always use TLS.

Authentication

All users (both print buyers and print operators) are required to have user IDs and passwords. User IDs are sometimes email addresses. Administrators can configure password rules to enforce custom password policies for improved security or convenience.

User Information

Basic user information, such as shipping and billing addresses, is kept in the database, and it is dependent on the server and network security of the system deployment. Credit card numbers, however, are not stored in the EFI database, but are instead passed through, encrypted, to a supported payment gateway (such as Payflow Pro, CyberSource®, or Ingenico ePayments).

Cookies

The system depends on the use of temporary cookies to maintain the relationship between the user's browser and the application to maintain the contents of the shopping cart. Any user who prohibits even temporary cookies will not be able to use the service.

Cloud Application Security: General Overview

Although all organizations want their assets to be secure, no two organizations have precisely the same security requirements. Security requirements differ based on the nature of a business, the industry in which it operates, and its specific business model. Although all security issues are important, every organization will assign a different degree of importance to each issue and choose a solution that best meets its particular security needs.

When you choose to have EFI provide your company with a cloud solution, the following considerations are crucial to your secure implementation.

Security for Cloud Applications

Strong, enterprise-wide security demands solutions and technologies made from proven, robust components. EFI offers a comprehensive security infrastructure that extends through its hosting facilities and out to your own organization. EFI cloud applications and the EFI Cloud Services group offer a solid, reliable foundation.

With cloud applications, EFI assumes responsibility for many aspects of the security of the implementation.

Roles and Access Privileges

Employees inside the organization can be segmented by role. For example, your sales team may be prevented from accessing production schedules, while everyone but accountants is restricted from accessing finance data. Unauthorized personnel, of course, should have no access. This is accomplished by application features, infrastructure design, and operational security.

Availability

Users of Internet applications demand high availability and optimum performance. All users – employees, customers, and partners – need predictability and availability. Protecting your IT assets from degraded performance, unplanned outages, and unauthorized access is essential to maintaining the high service levels users expect.

Consistency

Users also expect systems to perform in a consistent manner. If software or hardware exhibits radically different behavior, it could signal corrupted applications or data. Security utilities and mechanisms can check servers for application and data consistency. The monitoring and maintenance of your system configuration promotes reliability and availability.

Access Control

Unknown and unauthorized individuals can cause damage to your IT assets. If a system is attacked, network security administrators must determine how access was gained, what damage was done, and who accessed

the system. Recovering from such episodes can require considerable time and expense. For these reasons, access to servers, data, and other IT resources must be strictly controlled by user role, permission, and authorization.

Data Confidentiality and Encryption

Information must not be read or copied by anyone who has not been explicitly authorized to do so. Data confidentiality includes protecting information that is on a server or is traveling across a network, or protecting seemingly harmless data, which can be used to infer confidential information – the internal IP address of a mail server, for example. Encryption ensures confidentiality by making the data meaningless to anyone who is not authorized to read it.

Authentication

Clients need some way of verifying that the server they are communicating with is a valid server. Similarly, servers need to know that the clients are valid. Various levels of authentication are possible, from simple login-password pairs to token cards and biometric mechanisms. The authentication of clients and servers is a fundamental component in allowing access to specified services.

Security for Payment Processing

Certain EFI applications incorporate an optional credit card payment gateway module that works in conjunction with supported payment gateways such as PayFlow Pro, Ingenico ePayments, or CyberSource. A payment gateway simplifies the security and processing of payments online. Not only does a gateway make it fast and easy for your customers to purchase your goods and services on the Web, it also frees you from point-to-point payment solutions that are difficult to integrate. The combination of an EFI application with payment gateways provides the benefits of an integrated payment platform designed specifically for the Internet. As a result, your site can support multiple payment methods including credit cards, corporate or institutional purchase cards, debit cards, electronic checks, and ACH transfers. It provides you with back-end connectivity to all leading payment processing networks. Designed for scalability and reliability, these gateways can process large numbers of transactions simultaneously to ensure that your customers are not kept waiting and that no transactions are lost or delayed during the buying process.

Credit card information is sent using TLS (Transport Layer Security) encryption to secure transaction information. Standard processing level anti-fraud features such as AVS and CSC are included. When a customer visits your site and makes a purchase, the transaction data is passed securely from your storefront to the payment gateway (such as Payflow Pro) which, in turn, routes the transaction through the financial network to the appropriate bank, ensuring that your customers are authorized to make their purchase. In most cases, the credit card payment gateway module will work with your existing merchant account.

Cloud Application Security: Detailed Review

This section provides detailed information related to the security of cloud-based applications hosted by EFI. It addresses questions related to a number of such EFI applications and summarizes the security in place for these. Most of the applications provide additional or stronger measures but, significantly, EFI's approach to security is pervasive and implements the notion of "defense in depth."

Hosting Locations

The hosting takes place in North America and Europe.

North America Primary Facility

EFI
40 24th Street
Pittsburgh, PA 15222
USA

North America Secondary Facility

Expedient Data Center
701 Congressional Blvd #100
Carmel, IN 46032
USA

Europe Primary Cloud

Amazon Web Services
Region: AWS (London)
Availability Zone: eu-west-2a (euw2-az2)

Europe Secondary Cloud

Amazon Web Services
Region: AWS (London)
Availability Zone: eu-west-2b (euw2-az3)

Security and Privacy Training and Controls

EFI hosting staff undergo criminal and professional background checks. EFI requires and maintains non-disclosure agreements (NDA) with employees, contractors, and third parties involved in hosting operations or with possible access to sensitive information. Ongoing training of operations personnel in the matters of security and privacy occurs regularly.

Physical Security

Access to the hosting facilities is strictly controlled and monitored, for example, through security cameras, alarms, proximity access systems, and security guards.

Environment and Power

Hosting facilities include temperature and humidity controls, fire detection and suppression systems, UPS units to condition power, backup generators, and redundant systems.

Communications

Each hosting facility has multiple access entry points for routing data, as well as access to multiple communications providers (ISPs) to allow load balancing. In addition, the ability to disconnect from one ISP in case of an attack provides an additional element of security.

A highly-virtualized, monitored, and redundant cloud environment allows EFI to deliver seamless service of its hosted applications.

Production networks are isolated from EFI corporate networks as well as the public Internet. Such a design is sometimes called a DMZ (for “demilitarized zone”). EFI secures resources and information assets based on a number of criteria using segregated networks.

Backups

EFI uses a number of backup procedures to ensure the availability of the site. Data backups occur nightly. Encrypted copies of backups are stored offsite in a suitable third-party facility or cloud. Secure transmission occurs immediately to disk-based backup appliances which allow for speedy recovery.

Site and Fault Monitoring

Operations are monitored from five independent stations. Operations personnel are notified immediately of conditions that could impact service. Additionally, the application itself reports errors via email. The types of monitoring range from “ping and pipe” on ISP connections and servers to a user experience test on each server. Monitoring tools regularly log into the Web site (on each server), navigate through screens, and log out to ensure timely and accurate performance. An escalation process is in place to ensure that all alerts are resolved efficiently.

Network systems, including providers, firewalls, load balancers, and switches, are configured redundantly. Fault-tolerant servers are used throughout. Hardware load balancers allow the use of multiple Web and application servers to provide rapid recovery from failures (*i.e.*, if a fault-tolerant server fails or needs to be taken out of service). Database systems use highly redundant and fault-tolerant hardware and clustering technologies.

Logical Data Access Control Based on “Least Privilege”

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. Access to back-end systems for non-operations personnel is allowed only in cases where it is reasonably required to assist customers or to isolate a defect. Such access is almost exclusively a limited, read-only view with no system control. System and database access is allowed only on a per user basis. Networks and systems passwords are known to only the bottom two tiers of the EFI hierarchy. The top three or more tiers may direct action in compliance with policy but are not empowered to directly execute security-sensitive operations.

Operational controls are independently audited annually for fiscally sensitive data and procedures.

Authorization and Protection Controls

User, system, and data access controls

Users are authenticated for every page in the system. Different types of authentication are possible, depending on the implementation. Access to files is accomplished via file server security layered underneath application-moderated access. That is, the application allows users access at one level, and the application itself has restricted access at a lower level. The system accesses all resources via a single well-known local account on the server that hosts the software.

Management of user rights, privileges, and/or entitlements

A user profile contains information about the user and the user’s status. The first profiles created are for those people in your business who need access to the system, such as the administrator, a secondary administrator, and operators who produce print jobs at a location. The administrator then assigns each user to a specific facility. Typical user attributes include: *Company* (the account the user belongs to), *Group* (the group the user belongs to), *Facility* (the print facility the user is assigned to), *Price Sheet* (the price sheet associated with the user’s billing entity), and *Status* (active or inactive).

Group access to Web pages

Security is enforced in most EFI software through group access to Web pages. After groups are defined, users can be placed into the appropriate group with access to different options and features. In general, the number of groups is unlimited, and additional users may register on the home page of the Web site. The administrator may configure the registration page by choosing from a list of pertinent questions that may or may not be designated as required information fields. The system may automatically send users a system-generated password or users may choose their own passwords and gain immediate access to the site.

Data Transfer Control, Encryption, and Key Management

All EFI applications implement TLS encryption around security-sensitive traffic, such as pages dealing with login and password information. For most applications, whole-site encryption can be enabled. This encryption in transit provides critical protection for your data as it flows across the public Internet.

Encryption at rest is also utilized for data behind EFI’s firewalls. EFI delivers storage/volume encryption so that virtual machine,

database, file, and snapshot information and metadata are encrypted. System Downtime and Business Continuity

Availability, or “uptime,” for most EFI cloud customers has exceeded 99.8%, excluding announced events for maintenance.

EFI has two categories of system downtime: planned and unplanned. Every effort is taken from development though delivery to ensure outages are brief and infrequent.

Planned outages

EFI endeavors to perform routine and required maintenance during off-peak hours. During these times, the systems may be unavailable or unstable. Exceptional outages are announced via email in advance of the outage.

Unplanned outages

To avoid unplanned outages, EFI utilizes redundant hardware, electrical, networking, and software technologies to minimize interruptions. By design, many maintenance operations can be performed with no interruption in service. Various components are monitored around the clock from points around the globe. Problems often are detected, isolated, and resolved without customer impact.

When an unplanned interruption occurs, operations personnel respond 24/7. Typically, information from customer service or monitoring systems is available to operations personnel within seconds.

Proactive Maintenance

EFI performs monitoring, backups, patching, virus protection, account maintenance, tuning, troubleshooting, security, and the like to proactively preserve the stability of the environment. These services are provided according to procedures written and tested by certified personnel.

The EFI change management process specifies the persons who perform each change, and these are subject to the review process. EFI retains experienced and qualified personnel with expertise in the hardware and software platforms supported. In addition, support contracts are in place for critical elements of the environment.

Vulnerability and Threat Management

New threats are always emerging. EFI practices security-by-design during the development process. QA teams regularly check for potential problems in release candidate software. EFI also practices continuous vulnerability managmenet. Security, virus, and operations teams monitor public news sources and subscribe to email bulletin services for alerts. Operations teams also review software error logs for suspicious activity. If a vulnerability is discovered in third-party software, available patches are tested and deployed. If the vulnerability is discovered within EFI software, a defect is logged, QA and development teams are notified, and appropriate management attention is drawn to the problem.

In addition, an Intrusion Protection System (IPS) intercepts all traffic incoming from, and outgoing to, the Internet, and processes and profiles the traffic on site. This system will actively terminate suspicious traffic and activity it detections. Further Host Intrusion Detection System (HIDS) software is deployed on each host.

Anti-Virus and Malicious Code Controls

EFI hosting facilities include border firewalls; intrusion detection systems; real-time centralized analysis of system logs; router access control lists; active virus filtering at the corporate border; anti-virus software deployed on all production, management, and pre-production systems; automatic pattern file updates; and centralized virus reporting (including 24/7 alerts). Anti-virus software is implemented on workstations, servers, and email servers to address viral/malicious code. The anti-virus software is configured to prevent users from disabling it and is configured to perform scheduled automatic scanning of workstations and servers.

If a suspicious activity occurs, or a noteworthy threat is present, software and pattern files and updates are triggered manually by the virus team. Automated processes are in place for workstations, servers, and email servers - updates are pulled to a central pattern validation station and available for all workstations within three hours.

In combination, these measures allow real-time situation handling on all common channels of propagation.

Summary

The information provided in this white paper was intended to provide a detailed overview of security issues related to EFI cloud applications. The applications and the hosting apparatus are ever-evolving in the interest of providing better functionality and security to EFI clients. The specifics discussed are changed and updated from time to time as EFI releases new versions of its software. For more information about application configuration options, deployment configurations, and additional capabilities, contact your EFI sales representative.