VASION®

Virtual Appliance Overview

A white paper explaining the benefits, architecture, and operational details of Vasion Print's latest customer-hosted solution

Table of Contents

Vasion Overview

Vasion earned its reputation by providing a feature-rich, secure, and easy-to-use serverless printing infrastructure with their Vasion Print product. Vasion Print converts legacy print environments into highly available, centrally managed direct-IP printing systems. The Vasion Platform offers Vasion Print for simplified end user printing, Vasion Output for business critical printing, and Vasion Automate for business process automation.

With Vasion Print, there's no need for Group Policy Objects (GPOs) or time-consuming scripting to deploy and manage printers and drivers. Print jobs go straight to the printer via direct IP, confidential data remains local, and WAN traffic is minimized.

There are two versions of Vasion Print. One is a true SaaS implementation that eliminates the need for traditional print-server infrastructure, hardware resources, licensing, or maintenance. The other is an easily updated virtual appliance for on-premises use with equivalent functionality.

This paper describes the benefits, architecture, and security details of the Vasion Virtual Appliance, which has replaced the company's traditional on-premises version known as Web Stack.

What is the Vasion Virtual Appliance?

The Vasion Virtual Appliance (VA) is part of Vasion's on-premises platform. The Virtual Appliance is typically a great fit for companies that want the benefits of Vasion's serverless printing infrastructure but need tighter control over their print environment.

The VA is a fully integrated solution that supports:

- VMware (OVA, VMDK)
- Hyper-V (VHD)
- AWS (AMI)
- Google Cloud Platform (VMDK)
- Azure

This solution helps customers maximize their investment in virtual infrastructure designed to reduce unnecessary hardware, software, and ongoing maintenance costs.

The VA has been called "SaaS in a box" because it is a parallel delivery system for the same application. The VA is a complete, unitized solution that's ready to install, including a server OS, web services, network environment, and the Vasion Print application.

The VA includes a timely and easy update system that lets customers get the latest features and improvements. Features become available soon after they are pushed to Vasion Print SaaS.

Key components include: (1) a self-contained management server, (2) a small app that's installed on every workstation (known as "the Client"), and (3) an enhanced client for additional services that's a shared resource (known as the "Service Client"). The latter is installed on a workstation that remains powered on.

Virtual Appliance: A Closer Look

Moving to a VA provides several important benefits. These are derived from new technologies, the architecture itself, and a more timely updating process.

- As preconfigured, pretested solutions, VAs are easier to evaluate, quicker to deploy, and less expensive to maintain. They reduce the costs and complexities associated with OS and hardware configuration, easing the burden on IT.
- New features are available more frequently and updates are easier. Application updates are available soon after they are pushed to the corresponding SaaS platform. Once the update is downloaded, the old version is detached from persistent storage, and the new one is attached.
- VAs are more secure on several fronts. Their low-profile operating environment is less exposed as an attack surface. The OS and platform elements are updated more regularly, reducing vulnerabilities. Developers gain tighter control because VAs provide content verification and integrity checking based on public-key infrastructure.
- VAs free up IT resources for more customer-oriented tasks such as training, support, and continuity of service. And, if something goes wrong, a VA is a single-vendor solution with one point of accountability.

The Virtual Appliance Architecture

The VA consists of the elements in Figure 1. These elements are explained in detail in the following paragraphs below the diagram:

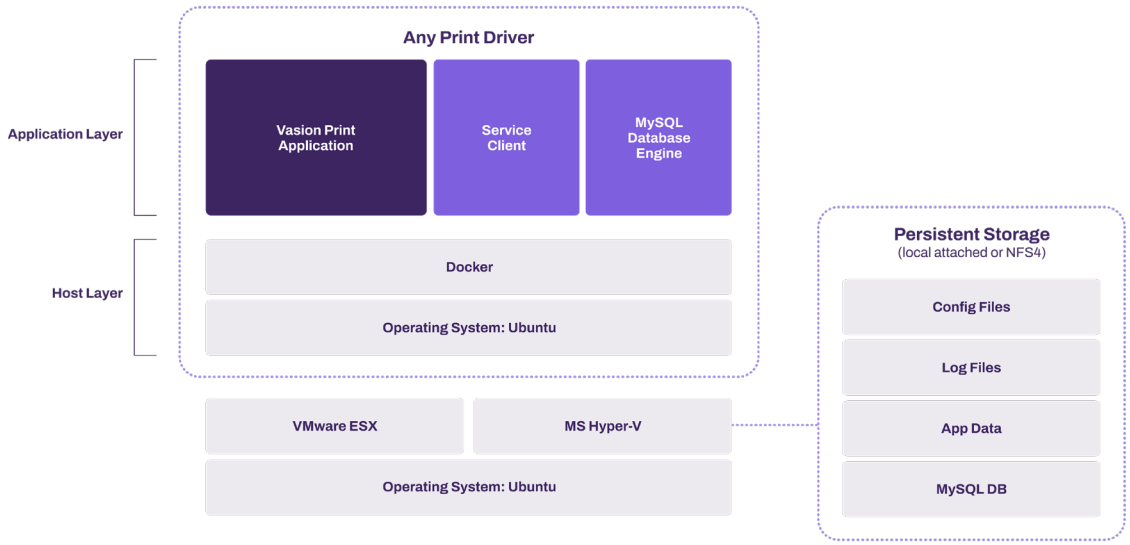

Figure 1: The Virtual Appliance contains an application layer and a host layer. In this (default) configuration, the MySQL database engine is inside the VA.

The Application Layer

The application layer, shown above, contains three parts: (1) the core Vasion Print application, which consists of microservices; (2) the Service Client; and (3) the MySQL database engine. If upgrades and/or bug fixes are available, a new application version is displayed in the Admin Console. These components are explained below:

The Vasion Print Application

The Vasion Print application is the heart of the product. The app provides users with a serverless printing infrastructure.

A single shared "code train" between the company's SaaS and VA solutions uses a series of discrete microservices. For example, the user microservice manages users and the authentication information received from an identity provider (IdP), whereas the queue microservice manages print queues.

Each microservice is self-contained, maintains its own data store, and can be updated independently. These services communicate with each other in well-defined and prescribed ways. Software designed this way speeds up application development and makes implementing new features and functionality easier.

An app that uses microservices runs more efficiently on multiple servers, where load balancing demands adjustments for transient spikes and steady increases over time. This approach also reduces downtime caused by hardware or software problems.

Vasion Print Service Client

The Service Client is an enhanced version of the Vasion Print Workstation Client. It facilitates communication between the Vasion Print Instance and user endpoints, enables advanced features, and ensures that confidential print data is kept local and secure. This is explained more in the Vasion Print Service Client section below.

MySQL Database Engine

MySQL is the database used by the Vasion Virtual Appliance. The MySQL engine is separate from the data store. It is containerized and installed on Docker, with the physical storage separated and outside the Virtual Appliance.

This allows the Virtual Appliance to be immutable, which means it cannot be changed but can be "destroyed" to make room for a new Virtual Appliance that is then spun up to replace it. The database is configured in one of two ways, as discussed in the Host Layer section below.

The Host Layer

This layer consists of Docker, a containerization solution, and Ubuntu, the operating system.

Docker

Docker is a container tool that uses OS-level virtualization, making it easier to create, deploy, and run applications. It packages up the application and its associated parts, such as libraries and other dependencies. Containers are run by a single operating system kernel and use fewer resources than virtual machines.

Within the VA, Docker is configured to act as a single-node swarm, which increases manageable container traffic.

The Hypervisor

A hypervisor is server visualization software that creates and runs virtual machines. It allows multiple operating systems to run independently on a single machine in a data center. Hypervisors encapsulate a guest version of the operating system and emulate hardware resources. They improve resource utilization and lower server costs.

VA Supports the following hypervisors and cloud Platforms:

- VMware ESXi
- Microsoft Hyper-V
- Google Cloud Platform
- AWS
- Azure

Persistent Storage – Option 1

In a default installation of the VA, the MySQL engine is containerized and installed on Docker within the appliance. The physical database resides outside the VA in persistent storage. Also stored there are the configuration, log, and app data files required by Vasion Print.

Persistent Storage – Option 2

As shown in Figure 2 below, a second option affords the Vasion Print customer more control over the database provisioning. Here we see the VA configured so the MySQL engine and database are held outside the VA. Along with local storage, the VA will support NFS4.

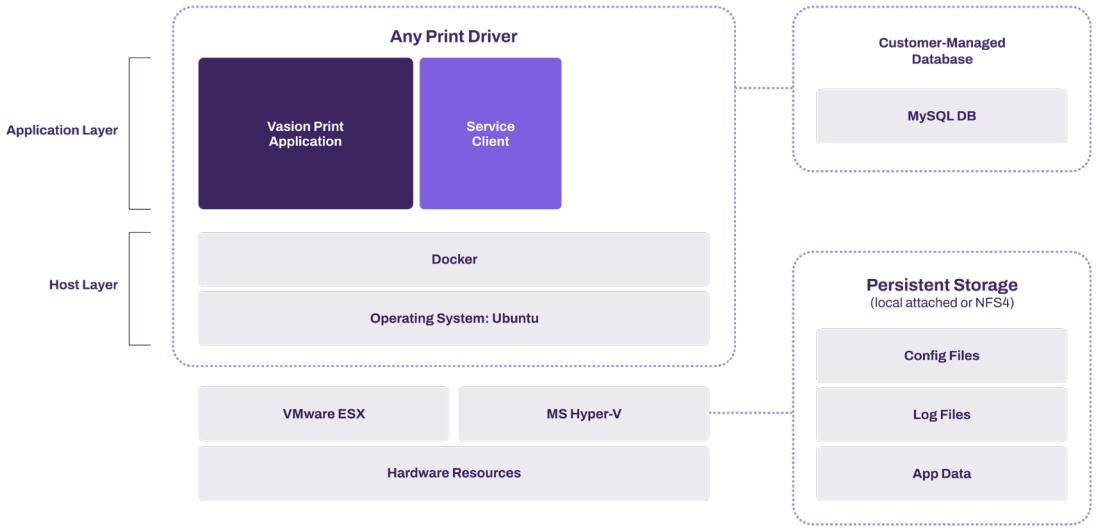

Figure 2: The Virtual Appliance with customer-managed MySQL database engine and data store outside the VA.

Upgrading the Virtual Appliance

As with all software systems, Vasion Print is updated to introduce new functionality and/or fixes. Because the Virtual Appliance includes an operating system, vulnerabilities that crop up in the OS must be addressed. This requires an upgrade to the host layer.

The architecture of the VA allows for the following upgrade scenarios:

1. **Update button in the Admin Console:** The application layer is updated, including the Vasion Print application, Service Client, and the MySQL database engine.
2. **The entire Virtual Appliance is replaced:** This includes the application layer, the host layer, OS, etc.

Consolidated updates for the VA will occur quarterly, while SaaS deployments for Vasion Print will continue on a more frequent cadence. The ability to download a new VA quickly, load it, spin it up, and then attach it to the persistent storage minimizes down-time and ensures minimal business disruption.

Upgrades are executed at the administrator's discretion. An update button within the Vasion Print Admin Console will show what updates are available at any given time.

Differences Between Vasion Print's SaaS and VA

There are three major differences between Vasion Print's SaaS solution and its on-premise (VA) solution:

Hosting Location and Admin Control

Vasion Print SaaS is a well-architected AWS solution hosted in several geographic public cloud regions. No additional servers need to be hosted in your private cloud or data center. Because it is a true SaaS offering and is secured by AWS, the platform does not offer IT administrators direct access to the database that houses the instance information.

The Vasion Print VA is a self-contained preconfigured VM image that is hosted on the customer's hypervisor—either in an on-premise data center, a private cloud data center, or a public cloud data center. Because the customer hosts it, they have direct access to their VA instance database and related information.

Multi-tenancy and the MSP/SMB Marketplace

Because Vasion Print is built on a scalable AWS platform, the company can offer a solution for multi-tenancy using a single management console. This solution has been designed with managed service providers (MSPs) and smaller businesses in mind. The Virtual Appliance is designed to support one customer instance per VA.

Different Upgrade Systems: Push versus Pull

Vasion Print SaaS follows a frequent update delivery model, automatically deploying new features and fixes to SaaS instances.

There are two methods for updating the Virtual Appliance. First, a full-replacement update method involves detaching the persistent storage disk and replacing the Virtual Appliance with the updated version. Second, the VA allows partial updates, which are accessible via an option in the Tools menu.

Virtual Appliance Operational and Security Details

This section explains the operational and secure communication protocols that apply to the Vasion Virtual Appliance.

Vasion Print Instance Client Communications

Vasion Print uses an instance client model to manage and deploy printer drivers and default printing preferences. The client is a small app that's installed on end user workstations. It communicates with the Vasion Print instance over HTTP or, with a validated certificate, HTTPS using TLS. HTTP and HTTPS communication paths use an OAuth2 security token that is granted when the client is installed.

Upon logging into the workstation (and on a scheduled interval), the workstation client uses the OAuth2 secure token to broker requests made to the Vasion Print instance. The client sends an HTTP/HTTPS request to the Vasion Print instance to see if any activities are assigned to the workstation or the user. If the workstation client does not have a valid OAuth2 security token, communication with the Vasion Print instance is denied, and the user is told to contact their administrator for a new code.

Once the workstation client has a valid OAuth2 security token, all communication, including driver and profile installs/updates, client updates, metadata reporting, and client check-ins, is secured over HTTP/HTTPs and TLS. This eliminates the need for any additional open ports in the firewall.

Expiration lengths are assigned to authorization codes for OAuth2 security tokens. Authorization codes not used within the allotted time become invalid, and a new one must be generated. The administrator can revoke an OAuth2 security token for any workstation if needed. In this case, the workstation client asks for a new code. Once a new code is entered, the client is granted a new token, and the authorization code expiration timer begins again.

The Vasion Print Admin Console and Driver Deployment

Printer drivers are uploaded to the Vasion Print instance using a manual upload process or via an automatic method that's set up when Vasion Print is configured. At start-up, Vasion Print can import drivers and profile settings from one or more print servers, which will be decommissioned later. For this to work, an OAuth2 security token is obtained using the authorization code for the workstation running the Vasion Print import tool.

The Vasion Print Admin Console is used to specify that a driver needs to be installed by the workstation client. When a client checks in and receives this instruction, it scans the local workstation first for the specified driver. If unavailable, the client downloads the driver from the Vasion Print instance or a designated driver cache. The driver is then installed using system service privileges on the workstation. Only drivers that are signed by a trusted certificate authority (typically the printer manufacturer) can be installed by Vasion Print. The workstation client configures the driver according to the profile defined in the Admin Console.

When printer drivers are downloaded from the Vasion Print instance, they are sent over an encrypted port (443) using HTTPS or HTTP and are confirmed with hash verification. Drivers can also be stored in a local cache using a distributed file system (DFS), a file share, or a workstation that's always available. The client installed on a designated cache manager must first receive an OAuth2 security token to enable communication. Once the token is received, obscured printer drivers are copied to the file share from the Vasion Print instance over port 443 or 80. Other workstation clients in the environment retrieve printer drivers from the file share using port 445, a standard means of communication on a Microsoft-based LAN.

Print Jobs Remain on the Local Network

Print jobs are sent directly from Windows, macOS, and Linux workstations to the printer via direct IP using port 9100 by default or as defined in the Vasion Print instance. Vasion Print's Chrome OS Client Extension sends print jobs over IPP using port 631.

For reporting purposes, only metadata for print jobs is sent via HTTP/HTTPS to the Vasion Print instance and a valid OAuth2 security token is required for this communication. This metadata includes print job date, time, user, originating workstation, printer name, document title, page size, and page count. The display of document titles can be disabled in the Admin Console.

Communication with Microsoft Active Directory

Vasion Print employs **identity provider services (IdPs)** services to authenticate and authorize users, groups, and computers for various optional features. These include Admin Console login access, pull printing, and mobile printing. Configuring Vasion Print for Active Directory (AD) integration requires the IP address or hostname of the primary and optional secondary LDAP servers and the port being used are 389 or 636.

The Vasion Print instance uses read-only permissions to access the AD server. Each time an authentication or AD membership is required (e.g., by mobile printing, email printing, control panel platform AD sync, or badge ID if stored in AD), Vasion Print requests AD using a BIND service account. The BIND account information is encrypted and stored in the Vasion Print database. The administrator can use a BIND service account with read-only permissions for added security.

When using Vasion Print Secure Release Printing, some release mechanisms require the use of the LDAP Sync function. These include username/password, user ID/PIN, and badge release. A Vasion Print utility synchronizes AD user names, badge IDs, PIN codes, and email addresses within the Vasion Print user microservice. This data is synchronized using the BIND account and is accessed over port 443 by the Service Client or printer control panel application during user authentication at the printer.

The client installed on the end user workstation does not connect directly to the Vasion Print instance for user authentication. Instead, the client authenticates against Active Directory using Active Directory Service Interfaces (ADSI) from a Windows workstation. It uses Kerberos tickets from a Mac or Linux workstation.

Communication with Cloud Identity Providers (IdPs)

If Vasion Print is configured to integrate with a cloud-based identity provider (e.g., Azure AD), user-identity information managed in the IdP console is synchronized with Vasion Print using SCIM (System for Cross-domain Identity Management). Updates that flow from the IdP to Vasion Print occur in real-time.

In addition, logins to the Vasion Print instance are facilitated through the IdP using the Security Assertion Markup Language 2.0 (SAML 2.0). Synchronized identity information provided by the IdP is used to authorize access to the Vasion Print Self-service Installation Portal, the Vasion Print Admin Console, and authorized printer deployments. Enhanced security features such as multi-factor authentication (MFA) and single sign-on (SSO), if enabled, are handled by the identity provider. These capabilities improve authentication security and offer productivity advantages for end users.

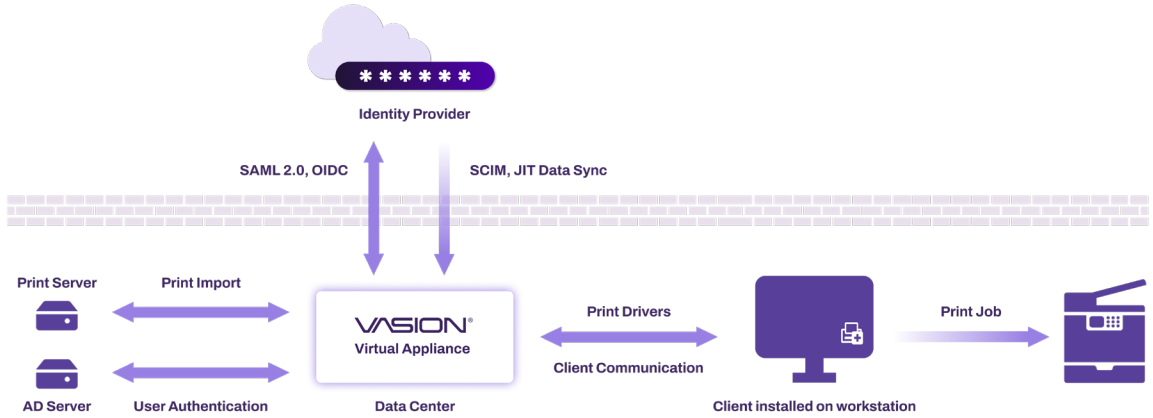

Figure 3: The Vasion Print communication paths for the Virtual Appliance and workstation client.

Vasion Print Service Client

Service Client functional overview

The Vasion Print Service Client is essential to Vasion Print's serverless printing platform. It is an enhanced version of the Vasion Print Client that's installed on Windows, macOS or Linux workstations. The Service Client facilitates communication between the Vasion Print instance and advanced Vasion Print features so that confidential print data remains on the local network.

Here's a list of features that rely on the Service Client:

- Simple Badge Release (for network printers without a console interface)
- Control Panel Application authentication (badge release, UserID/PIN)
- SNMP monitoring (when Service Client option is enabled)
- Email Printing (Standard, Direct)
- Installing a Control Panel Application on a printer
- Offline Secure Release
- Off-network Printing Gateway

How the Service Client is Configured

In the Vasion Print Admin Console, a Service Client object is created in the tree using the hostname or IP address of any Windows, macOS, or Linux workstation that is always on. The Vasion Print Client is installed on the designated workstation using the security process described earlier in this document. (See Vasion Print Instance and Client Communications.)

When the workstation client checks in with the Vasion Print instance, it detects that it's been designated as a Service Client, and the client OAuth2 secure token is used to retrieve a second OAuth2 secure token from the Vasion Print instance will be used to facilitate the upgrade.

The new Service Client then starts up the following processes according to the features that were enabled in the Vasion Print Admin Console:

- **Email Printing:** PrinterLogicServiceEmail
- **Control Panel App:** PrinterLogicServicePrinterApp
- **Offline Secure Release:** PrinterLogicServiceOfflinePrint
- **SNMP Monitoring:** PrinterLogicServiceSNMP
- **Simple Badge Release:** PrinterLogicServiceSimpleBadgeRelease
- **Off-Network Printing:** PrinterLogicOffNetworkServer
- **Identity Sync Service:** PrinterLogicServiceIdentitySync

Secure Release and Pull Printing

Secure Release and pull printing are available as part of Vasion Print's Advanced Security Bundle.

Vasion Print offers three secure printing methods:

1. **Pull printing** is a one-to-many option for held print jobs. Jobs sent to pull printers remain in a virtual queue on the workstation until the user authenticates and releases the print job to a pull-print-enabled printer.
2. **Direct Secure Release printing** is a one-to-one option for secure print. Print jobs can only be released at the printer they were assigned. Users must authenticate and release the job using one of the available release methods below.
3. **Offline Secure Release printing** allows users to initiate a job and then release it from a virtual pull print queue even after the device goes to sleep, logs out, or shuts down.

For Pull Print or Secure Release, the print job is rendered by the print driver and stored in a raw or binary format on the user's workstation in C:\Windows\System32\spool\PRINTERS\held\local, a secure folder location that only administrators have access to until the user goes to the printer and releases the job.

Offline Secure Release printing is different. The end user initiates the print job and then can shut down their laptop or workstation and receive the print job later. First, a copy of the print job is held on their workstation. In addition, a copy of the raw print job is sent to the Vasion Print Service Client over port 31989, where it is encrypted using an open SSL AES-256 algorithm. It remains encrypted on the Service Client and at rest in the C:\Program Files (x86)\Printer Properties Pro\Printer InstallerClient\ServiceClientStorage\PrinterLogicOfflinePrintApp\jobs\held.

When the end user goes to a printer to release the job, Vasion Print attempts to release the job that's held on their workstation. If the workstation is offline, Vasion Print contacts the Service Client to release its encrypted copy. In the latter scenario, the print job is decrypted on the service client uses Open SSL and sends it to the target printer.

Once the secure print job is released, the extra copy of the print job is deleted from either the user's workstation (once the computer is back online) or from the Service Client, depending on how the job was executed.

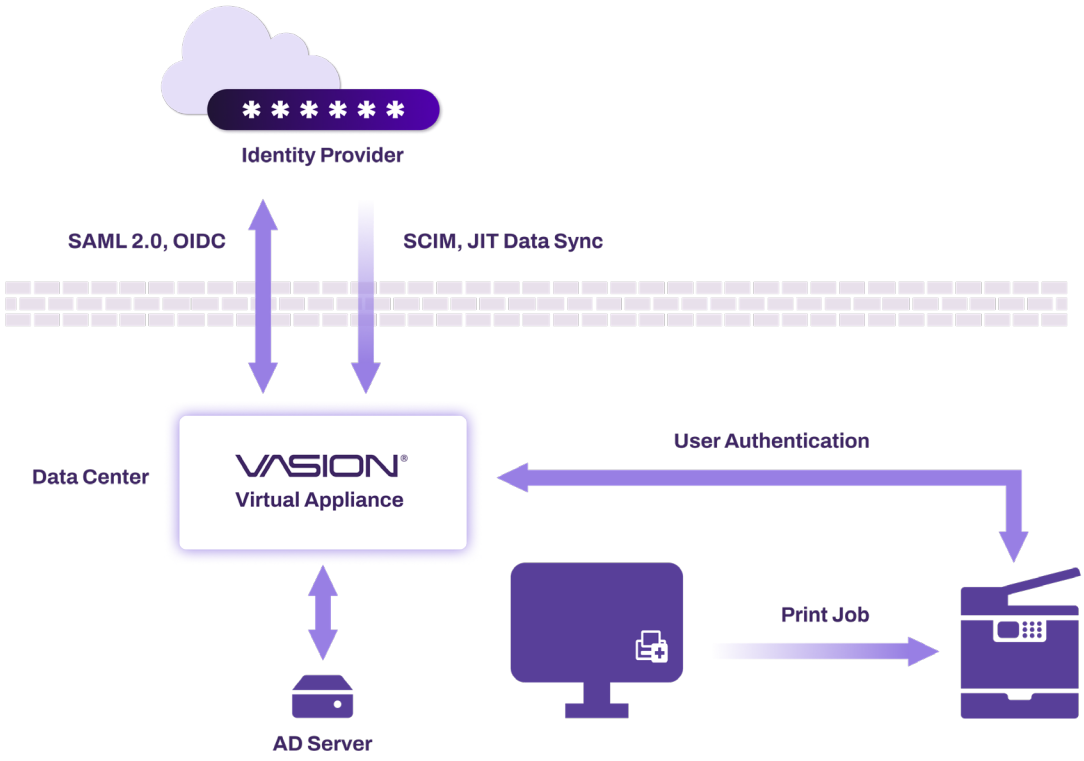

Figure 4: Communications flow for secure release printing. Users authenticate against either Active Directory or a cloud-based identity provider.

Methods for Secure Release Authentication

Vasion Print supports five mechanisms for releasing secure and pull print jobs:

1. **Touchless smartphone release with QR code support.** Releasing print jobs using our phone apps is convenient and avoids contact with the shared printer. Users can either view and release jobs from within the app or use the app's scanner to read a QR code on the printer. With QR codes, the printer is instantly identified, and printing begins, all in one step. Once the user's login credentials are entered into the app, they are stored for improved speed and convenience. What's more, it works with any network printer. Vasion Print's mobile apps are available on Apple's App Store and the Google Play Store.

2. **Control Panel Application (CPA).** Once the IT admin installs the Vasion Print application on a compatible network printer, end users can log in at the printer using their AD credentials or a user ID and PIN code. They are then shown any secure print jobs they sent to that printer and any pull print jobs waiting for release. When AD credentials are used for authentication, they are obfuscated and encrypted over port 443 to the Vasion Print instance and over port 636 to the AD server.

1. **CPA with badge/card reader.** When a supported printer has a built-in badge reader or is equipped with an optional badge reader, the user can swipe their badge for automatic authentication and skip entering AD credentials manually. End user badge IDs are stored in the Vasion Print database using the CPA badge registration process or in an AD attribute defined by the system administrator. When the badge is swiped, the badge ID is compared to IDs stored in the Vasion Print database (over port 443) or in Active Directory (over port 636). Once authenticated, the user can release a single job or all held print jobs to that printer as defined in the admin console.

2. **Simple badge release.** By connecting an ELATEC TCPConv 2 or rf IDEAS® E-241 network device and compatible badge reader to any network printer, the printer can be configured for fast, easy release of held print jobs. When the user swipes their badge on the reader, their badge ID is sent to the Vasion Print Service Client over port 31990. The Service Client then relays that information to the Vasion Print instance via port 443, where the ID is matched with a registered user account. Vasion Print authorizes that user and sends a release command to the ELATEC or rf IDEAS® device over port 443, and the user's print job is released. The administrator can configure Simple Badge Release to release the most recent or all held print jobs in a single motion.

3. **Web-based release portal.** From any web-enabled device (e.g., phone, tablet, laptop, PC), users can use their AD or IdP credentials to log in to the Vasion Print Release Portal. The portal shows their submitted pull/secure print jobs and lets them release one or more to the designated secure printer. Alternatively, they can select a destination printer from a list they are authorized to use. The Vasion Print Release Portal authenticates the user over secure LDAPS port 636 with the Active Directory server. If IdP is used, the user is redirected to their IdP portal for authentication, where their credentials are entered and verified.

Mobile Printing

The Mobile App for iOS and Android devices serves two purposes. First, as we described above, it is used to authenticate and release documents held for secure or pull printing. Second, the app allows users to print from their mobile device directly to virtually any printer on the organization's network. Mobile printing employs driverless printing via the Internet Printing Protocol (IPP).

Traditionally, setting up mobile printing requires network changes and configuring a broker between the mobile device and the printer. With the Vasion Print App, so long as the user's mobile device can access the same network where printers reside, no additional network changes are required. The mobile app uses the same set of Identity Providers supported by Vasion Print for any endpoint. The mobile user logs in using the same credentials they use on a workstation or laptop.

The app lets IT manage printer deployments for iOS and Android devices like they do for other endpoints. MDM deployment is supported, including preconfiguring the customer's Vasion Print instance URL. This simplifies the sign-in process for the end user and reduces help desk calls.

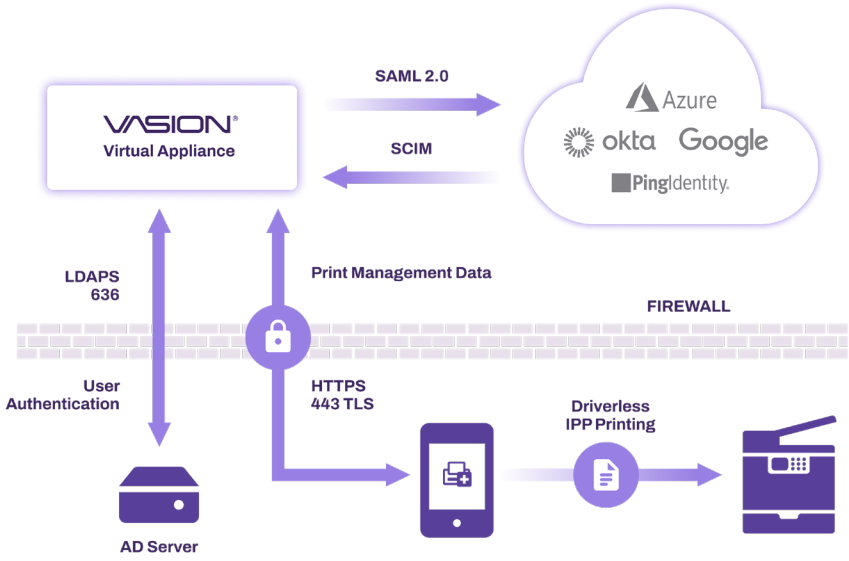

Figure 5: Mobile printing authentication, communication with the Vasion Print VA instance, and job routing to the network printer.

The diagram above illustrates the mobile printing process and pathways for authentication, communication with the Vasion Print instance, and routing for direct IP print jobs.

For direct mobile printing, the phone or tablet must be on the same Wi-Fi network as the printers. Documents are sent via direct IP and remain behind the firewall. With the Virtual Appliance, when using a mobile device to authenticate and release secure print jobs, the device must be on the same Wi-Fi network as the Vasion Print instance.

The app is available from the Apple App Store and the Google Play Store.

Email Printing

Vasion Print offers two email printing options: email printing and direct email printing. Both use the same configuration but handle print jobs differently.

With **email printing,** the admin creates or specifies a dedicated mailbox that the Vasion Print Service Client monitors. Any email sent to this mailbox is checked against AD using a BIND account to verify that the sender is authenticated. Emails that pass this test, including attachments, are retrieved from the dedicated mailbox by the Service Client using IMAP port 993 and converted to PDF. The print job is held on the Service Client until it's released to the target printer via direct IP over port 9100.

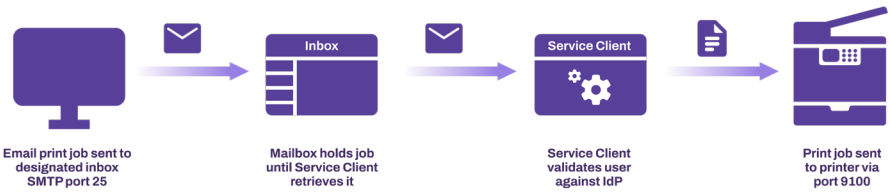

Figure 6: Email printing job flow using a Vasion Print VA-hosted Service Client and user validation against Active Directory or a cloud-based IdP.

With **direct email printing,** the admin creates or specifies a dedicated mailbox using a subdomain monitored by the Vasion Print Service Client. A mail-routing rule is created within the email service provider to route emails sent to the subdomain mailbox to the primary email-printing mailbox.

Any email sent directly to a printer's direct print email address is retrieved by the Service Client and checked against AD using a BIND account to verify that the sender is an authenticated user. It's also matched to the destination printer's email address according to its assignment in the Vasion Print Admin Console. Any emails that pass these tests, including attachments, are converted to PDF and sent from the Service Client via direct IP over port 9100 to the target printer.

Web Print

For unmanaged users like guests, Vasion offers Web Print, a secure, easy-to-use solution that can print through a web browser without accessing your network or downloading software. Once Web Print is enabled, Vasion provides a unique URL to a web portal. Companies can provide guests access to the web portal through a QR code, signage near the printer, or a link from staff members. Then, guests simply visit the company's web portal link on their device, enter their email address, and upload their document for printing. A print preview appears, allowing them to adjust formatting or settings (as configured by the IT administrator) and choose a printer from a dropdown menu Then, guests can choose to print immediately or receive an email with release instructions.

Web Print jobs can be held for Secure Release and help protect sensitive documents without compromising your network security. IT administrators have the ability to enforce all guests' print jobs to be held for secure release to manage the retrieval of confidential information. For secure release guest printing, Web Print utilizes Vasion's Off-Network Cloud Printing application, holding the print job in the cloud until released by the guest. Guests can release print jobs through the Control Panel Application (CPA) by entering a release code sent via email. All print jobs are encrypted during transit and at rest, using TLS for transmission and AES-256 encryption while stored in the cloud. This secure process eliminates the need for software downloads or access to your network, requiring only an email address and the web portal link for guests to print.

FIGURE 7: Web Print flow for guest users, detailing the process from document upload via a BYOD device to encrypted storage in Vasion's AWS, followed by release confirmation and the ONCP App downloading and printing the document.

Off-Network Printing

Off-network printing enables companies to provide convenient and secure printer access to employees, contractors, and partners on different networks. This capability is crucial to organizations adopting a Zero Trust architecture, using onsite contractors, or hosting traveling employees. Off-network printing provides visiting parties with an intuitive, highly available, secure printing experience.

Off-network printing allows users with internet access from any location to send print jobs to a printer behind the company firewall. In addition to the Vasion Print or VA instance, two other components make this solution work: the External Gateway and the Internal Routing Service

The External Gateway

The External Gateway receives off-network print jobs from remote workstations. In the Vasion Print-hosted model, the External Gateway is hosted as a service in AWS by Vasion Print. In the customer-hosted model, the External Gateway is hosted by the customer with an SSL (Secure Sockets Layer) certificate.

In addition, combined hosting models (known as hybrid models) can be used. The External Gateway uses port 443 to receive print jobs and uses WebSockets to transfer incoming print jobs to the Internal Routing Service. Print traffic is encrypted using the TLS (Transport Layer Security) cryptographic protocol.

The Internal Routing Service

The Internal Routing Service maintains a constant connection with the External Gateway to watch for print jobs. When the External Gateway receives a print job, the Internal Routing Service opens a new connection for that print job and downloads and delivers it to the designated printer.

Off-network printing has three configuration options: Vasion Print-hosted External Gateway with AWS, a customer-hosted External Gateway, and a hybrid model.

184852 | Mar 2025

Off-Network Cloud Printing (ONCP)

The difference between standard Off-Network Printing and its cloud-based remote printing approach is how print jobs are routed. It's in the name: through the cloud instead of requiring an on-premise Internal Routing Service running on the Service Client. Customer data is logically separated into Amazon Elastic File System (EFS) folders within the cloud. Jobs are sent to the Vasion Print ONCP External Gateway via an encrypted tunnel, where they are given a universally unique identifier to ensure that the job will route to the correct place.

Print jobs are held in the cloud storage microservice in an encrypted state until they are ready to be printed through the ONCP Printer Gateway. The ONCP app, installed on the printer, facilitates the traffic from the gateway to the printer using WebSocket connections (HTTPS or IPP). When the printer queue is ready for the job, the app communicates with the ONCP gateway and downloads the job data to print. Off-Network Cloud Print jobs can be held for Secure Release or pull printing and are stored in a cloud storage microservice until the release is initiated.

Conclusion

The Vasion Virtual Appliance is the latest generation of Vasion's on-premises platform. The VA can be installed on popular hypervisors and private cloud platforms to meet the requirements of a company's preferred infrastructure.

The Virtual Appliance is an excellent alternative for customers who prefer hosting their infrastructure rather than subscribing to Vasion Print SaaS. The VA mirrors all the features and benefits of the SaaS platform with the additional benefits of a simple infrastructure that is easy to install, manage, and update. It is an excellent pathway to true serverless printing in an on-premises environment.

Vasion Print offers printer deployment and management, print auditing and reporting, and centralized printer management from a web-based console. Concerning cost-effectiveness, Vasion Print has a proven track record for high return on investment. Customers report measurable gains from infrastructure reductions, improved IT efficiencies, optimized printing uptime/reliability, and lower helpdesk costs.

Try Vasion Print 30 Days Free