VASION®

Vasion SaaS Security: A Technical Overview

An operational summary of security design and communication protocols

Table of Contents

Vasion Overview and Scope of This Paper 3

The Vasion Print Instance and Client Communications 4

The Vasion Print Admin Console and Driver Deployment 5

Direct IP Print Jobs Remain on the Local Network 5

Communication With Microsoft Active Directory 6

Communication With Cloud-based Identity Providers (IdPs) 7

Vasion Print Service Client 8

Secure Release Methods 9

Direct IP Mobile Printing 11

Email Printing 12

Web Print 13

Off-Network Printing 14

Off-Network Mobile Printing 15

Off-Network Cloud Printing (ONCP) 16

Abbreviations Glossary 18

Vasion Overview and Scope of This Paper

Vasion earned its reputation by providing a serverless printing infrastructure that is feature-rich, secure, and easy to use. The Vasion solution offers two distribution models: a true SaaS implementation that eliminates the need for print servers, licensing, and maintenance, and a self-contained Virtual Appliance for on-prem and private-cloud use.

With the widespread adoption of cloud solutions, Vasion Print SaaS has become the preferred platform for new customers. It easily converts your printing environment into a highly available, centrally managed direct IP printing system. There is no need for Group Policy Objects (GPOs) or scripting to deploy and manage printers and drivers.

With Vasion Print, print jobs are sent directly from the workstation to the printer via direct IP so all print data remains local, even when using secure and pull printing features.[1] Print data only leaves the local network when using Off-Network and Off-Network Cloud Printing and is encrypted over HTTPS/SSL.

Key components of Vasion Print are a cloud instance (hosted in Amazon Web Services or Azure Cloud), a small app that's installed on every workstation (a client), and the Service Client.[2] The latter provides additional services for advanced features, such as Secure Release Printing and Off-Network Printing.

This paper provides security and operational details about Vasion Print SaaS. While there are overlapping similarities to our Virtual Appliance, the information below does not necessarily apply to on-prem installations.

1 In the default configuration, confidential data remains local and WAN traffic is minimized. In some advanced configurations described below, print data may flow through your secure cloud instance as it travels to a remote destination printer.

2 The Service Client can be installed on any Windows, Mac, or Linux workstations that remain powered on.

The Vasion Print Instance and Client Communications

Vasion is an APN Advanced Technology Partner. Our SaaS solution has passed the AWS Well-Architected review and renewal. In terms of hosting security, our software inherits all of the benefits of AWS Cloud Security and Azure Cloud.

Vasion Print uses an instance-client model to manage and deploy printers, and default printing preferences. The client is a small app that is installed on end-user workstations. It communicates with the Vasion Print instance over HTTPS using Transport Layer Security (TLS 1.2) and an OAuth2 security token that is granted when the client is installed with a valid authorization code.

Upon logging into the workstation (and on a scheduled interval), the workstation client uses the OAuth2 security token to authenticate requests made to the Vasion Print instance. The client sends an HTTPS request over port 443 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, it is denied communication with the Vasion Print instance, and the user is told to contact their administrator for a new authorization code.

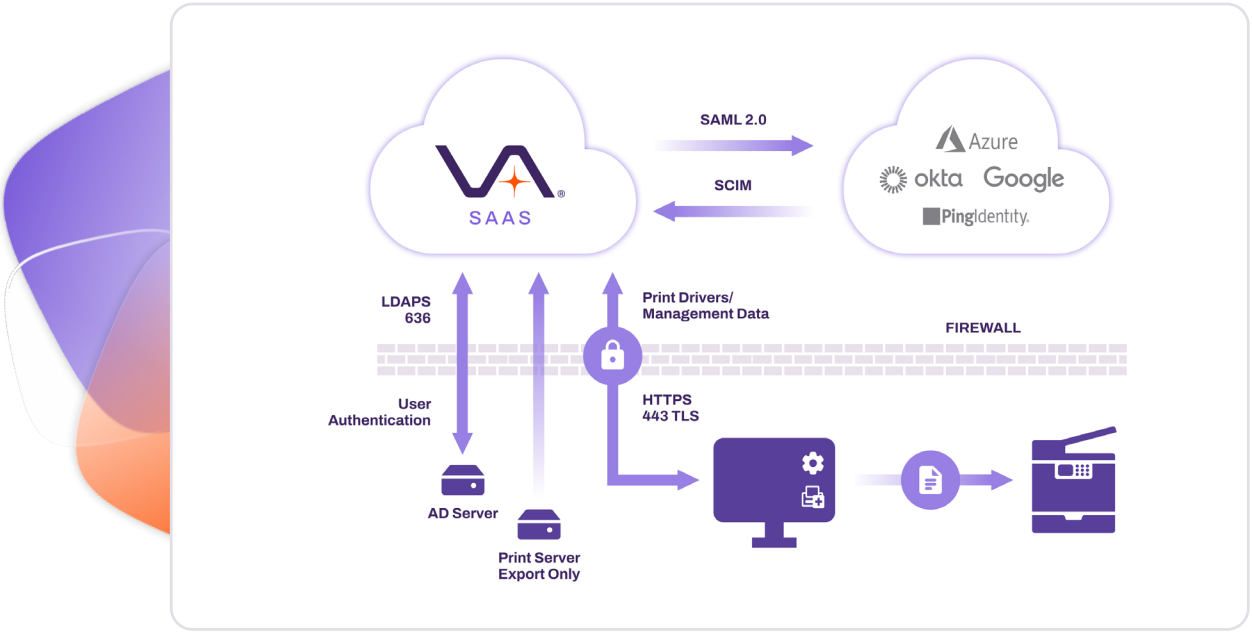

FIGURE 1: Vasion Print communication pathways for a SaaS instance, workstation client, and identity providers (IdPs).

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) are secured over TLS 1.2.

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

The Vasion Print Admin Console and Driver Deployment

Printer drivers can be added to the Vasion Print instance by a manual upload process. Vasion Print also provides a print server import tool, which can automatically import drivers and profiles from one or more print servers that will be decommissioned later.

The Vasion Print Admin Console identifies specific printer drivers that need to be installed by the workstation client.[3] When a client checks in and receives the list of drivers to install, it scans the local workstation first for the specified driver. If it's not available, 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) are installed by Vasion Print. The workstation client configures the driver according to the profile settings defined in the Admin Console.

When printer drivers are downloaded from the Vasion Print instance, they are sent over an encrypted port (443) using TLS 1.2 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. Workstations can then retrieve drivers from that local cache instead of downloading drivers from the Vasion Print instance. Printer drivers are downloaded from the Vasion Print instance over port 443, obfuscated, and stored on the file share. Other workstation clients in the environment retrieve printer drivers from the file share using port 445, which is a standard means of communication on a Microsoft-based LAN.

Direct IP Print Jobs Remain on the Local Network

Print jobs are sent from Windows, Mac, and Linux workstations directly to the printer via direct IP using port 9100 by default, or as otherwise defined in the Vasion Print instance. Vasion Print's **Chrome OS Client** Extension and the Mobile App (iOS & Android) send print jobs over IPP using port 631.[4]

For reporting purposes, metadata and basic Personally Identifiable Information (PII) such as user name, email, IP, and computer name for print jobs is sent via TLS 1.2 to the Vasion Print instance. This metadata includes print job date, time, user, originating workstation, printer name, document title, page size, and page count. Transfer of document titles can be disabled in the Admin Console.

There are situations where a workstation or mobile device does not have IP connectivity with the printer. This is where Vasion's Off-Network Printing and Off-Network Cloud Printing features can help organizations securely deliver print jobs across Zero Trust network boundaries. For details, see the Off-Network Printing section below.

3 The exception is the Chrome OS Extension which uses driverless Internet Printing Protocol (IPP) technology.

4 Due to OS security limitations, Chrome OS devices use the Vasion Print Chrome OS Extension instead of the Vasion Print Client. It provides similar functionality but cannot be promoted to a Service Client.

Communication With Microsoft Active Directory

Vasion Print can use one or more identity provider (IdP) services, including legacy Active Directory support, to authenticate and authorize users, groups, and workstations for a variety of optional features. These include Admin Console authentication, pull printing, and Mobile Printing.

Configuring Vasion Print for Active Directory (AD) integration involves several steps. Because the Vasion Print instance is outside the firewall, the IT admin must ensure that firewall rules allow access to Active Directory using the encrypted LDAPS protocol port (636).

When Vasion Print communicates with the AD server, communication is initiated from the Vasion Print instance within the Vasion Print Virtual Private Cloud (VPC) through a NAT gateway. This allows the customer to restrict the firewall rule to a single static source IP address that's based on the geographic region of the Vasion Print instance. The LDAPS request is secured using TLS 1.2 encryption to the customer's firewall, which then forwards the request directly to the LDAPS endpoint.

The Vasion Print instance uses read-only permissions to access the AD server. Each time an authentication attempt or AD group membership lookup is required (e.g., Email Printing, Control Panel Application authentication via AD username/password), Vasion Print reaches out to AD using a BIND service account. The BIND account information is encrypted and stored in the Vasion Print database. For added security, the administrator can use a BIND service account with read-only permissions.[5]

Some Vasion features, such as Email Printing and Secure Release Printing with the Vasion Print Control Panel Application, require use of the LDAP Sync function, which is enabled from the Identity Sync tab on the Service Client. LDAP Sync synchronizes certain attributes, such as AD user names, badge IDs, PIN codes, and email addresses, and stores them inside the Vasion Print user microservice. This data is retrieved locally by LDAP Sync using the BIND account and is uploaded to the Vasion Print instance over port 443 using TLS 1.2.

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 (ADSIs) from a Windows workstation. From a Mac or Linux workstation, it uses Kerberos tickets.

5 An alternative method for LDAP authentication is LDAP Identity Sync. By configuring the LDAP Identity Sync service on a Service Client, LDAP queries are kept behind the firewall and submitted to Vasion via HTTPS. Users' Active Directory passwords are not stored in LDAP, and are never synced to your Vasion instance.

Communication With Cloud-based Identity Providers (IdPs)

Vasion currently supports the following IdPs:

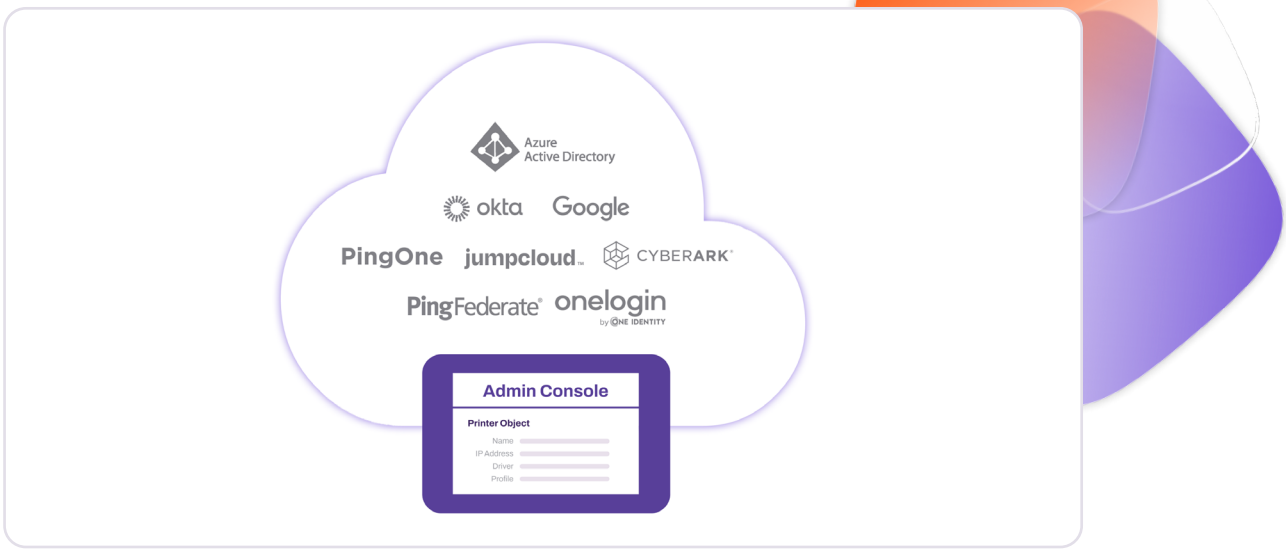

FIGURE 2: Vasion currently supports the identity providers shown above, and can add other IdP providers upon request.

If Vasion Print is configured to integrate with a cloud-based identity provider such as Okta or Azure AD, user-identity information managed in the IdP console is synchronized with Vasion Print. This is done using either the System for Cross-domain Identity Management (SCIM) or Just-in-Time (JIT) provisioning when a user logs in for the first time.

If the cloud-based IdP does not offer native SCIM support, Vasion Print has a similar service that runs on a Service Client and will synchronize the IdP users and groups. Synchronization between the IdP and Vasion Print ranges from nearly instantaneous for Okta to up to 40 minutes for Azure AD.

In addition, logins to the Vasion Print instance are facilitated through the IdP using the Security Assertion Markup Language 2.0 (SAML 2.0) or OpenID Connect (OIDC) in the case of Google. Synchronized identity information provided by the IdP is used to authorize the following:

- Access to the Vasion Print Self-Service Installation Portal
- Access to the Vasion Print Admin Console
- Print job release authentication
- The Vasion Print Client with the IdP user
- 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.

More information about how Vasion Print integrates with leading IdPs, including operational details and security standards, is available **in this white paper**.

Vasion Print Service Client

Functional Overview

The Vasion Print Service Client enables advanced features on Vasion Print's serverless platform. It facilitates communication between the Vasion Print instance and advanced Vasion Print features, and ensures that confidential print data remains on the local network in default configurations.

Features that rely on the Service Client include:

- Off-Network Printing
- Printer Control Panel Application (CPA) installation
- Control Panel Application authentication (badge release, User ID/PIN)
- Simple Badge Release (for network printers without a console interface)
- SNMP Monitoring (when Service Client option is enabled)
- Email Printing (Standard, Direct)
- Identity Sync Service (for IdPs without native SCIM support)
- Offline Secure Release for Windows endpoints

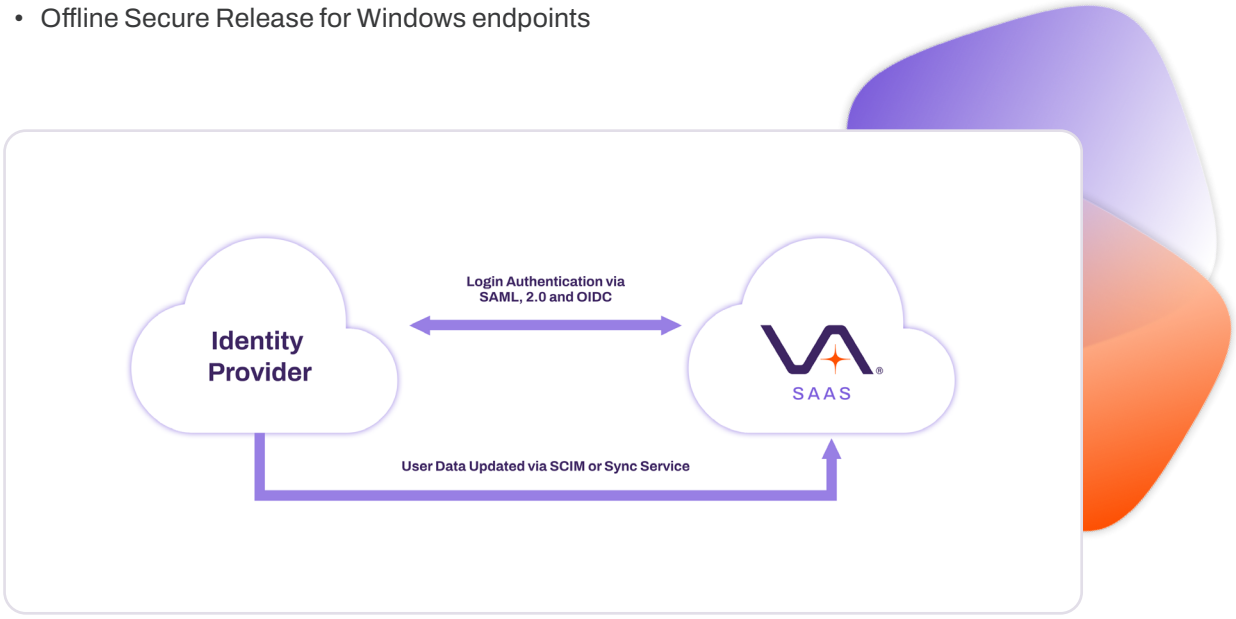

FIGURE 3: SCIM, OIDC, and SAML 2.0 in the Vasion Print integration.

How the Service Client Is Configured

Configuring a Service Client is a three-step process. First, in the Admin Console a Service Client Object is created in the tree using the hostname or IP address of any Windows, Mac, or Linux workstation that is configured to remain on. Second, the Vasion Print Client is installed on the designated workstation using the security process described above in the *Vasion Print Instance and Client Communications* section. Third, when the client checks in with the Vasion Print instance, it detects that it's been promoted to a Service Client, and it starts processes for any of the advanced features that were enabled. The client OAuth2 secure token is used to retrieve a second OAuth2 secure token from the Vasion Print instance.

Here's a list of the available Service Client processes:

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

Secure Release Methods

Vasion offers three secure printing methods:

- Pull printing (a virtual printer queue where the user decides later where to pick up the job)
- Secure Release Printing (a specific printer is configured to receive confidential print jobs)
- Offline Secure Release Printing (a job is initiated, the originating workstation goes offline, the job is printed later)

In the **pull-printing** scenario, the user prints to a secure virtual pull printer that holds the job on the user's workstation until they are ready to authenticate at the printer of their choice and receive their output.

In the **Secure Release Printing** scenario, the administrator designates a physical printer as a secure device. When a user prints to one of these printers, they get a prompt asking if they want their job held, or if they want it released immediately. The prompt is optional, and printers can be configured to always hold the job or to always release. If they opt to have the job held, they go to the designated printer and authenticate to release their output.

Either way, the print job is rendered by the printer 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 is restricted to administrators until the user goes to the printer and releases the job.

With **Offline Secure Release Printing**, the user initiates the print job and then has the option to 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 Service Client over port 31989, where it is encrypted using an open SSL AES-256 algorithm. At rest, it remains encrypted on the Service Client in the C:\Program Files (x86)\Printer Properties Pro\Printer Installer Client\service-offline-print\jobs\held folder.

When the end user goes to a printer to release the job, Vasion first tries to release the job held on their workstation. If the workstation is offline, Vasion contacts the Service Client to release its encrypted copy. In the latter scenario, the print job is decrypted on the Service Client using Open SSL and sent 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.

Offline Secure Release Printing on a local network is supported for Windows endpoints. Off-Network Cloud Printing, allows Offline Secure Release Printing in which the originating workstation is on a different network than the destination printer. This is especially useful for Zero Trust environments.

Methods for Secure Release Authentication

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

1. **Smartphone Release with QR code assist.** Our Mobile App is available on the Google Play Store or the Apple App Store. Once installed, the user enters their Vasion Print instance URL and Active Directory or IdP credentials. When authentication is complete, available secure and pull print jobs are shown on their screen. Communication between the app and the Vasion Print instance is over HTTPS using port 443.

   With pull printing, users can scan a QR code on a nearby printer to identify the desired output device. When the user uses the app to release the job, Vasion Print tells the user's workstation client, using port 443, to release the job. QR codes work with all printers and are a quick and convenient way for users to identify a printer without having to know its name.

2. **Control Panel Application (CPA).** Once a Vasion Print CPA is installed on a compatible network printer, users can log in at the printer using their AD credentials, User ID and PIN code, or a release code from their email. They are shown any held jobs waiting in the pull printing queue, and any jobs specifically directed to that printer for Secure 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. IdP authentication on the CPA currently supports PIN code and badging, but not username and password.

3. **Control Panel Application (CPA) with badge/card reader.** When a supported printer has a built-in badge reader—or is equipped with an optional badge reader—users can swipe their badge for automatic authentication. Badges and PINs can be collected using an active LDAP connection or the Vasion Print LDAP Sync feature, which removes the need for a firewall rule. End user badge IDs are stored in the Vasion Print database using the CPA badge registration process or in an 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.

4. **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(s) are released.

   The administrator can configure Simple Badge Release to release either the most recent, or all, held print jobs in a single motion. This feature is compatible with most printer models but requires the purchase of badge reader devices. Some administrators may prefer using smartphone release with QR code assist to avoid extra hardware costs

5. **Web-based Release Portal.** From any web-enabled device (i.e., phone, tablet, laptop, or PC), a user can use their AD or IdP credentials to log in to the Vasion Print Release Portal. The portal shows their held print jobs and lets them release one or more to the designated secure printer. Alternatively, they can select a destination printer from the same interface. The release portal authenticates the user over 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.

Direct IP Mobile Printing

Mobile devices are everywhere and, depending on the demands for computing power, have even become the "workstation" of choice for some users and environments. In the past, mobile printing often required printers with special features, cloud printing services, or configurations that could not be managed like other endpoints.

The Mobile App for iOS and Android treats the mobile device like any other endpoint. With the app, users can *print natively* using the same direct IP approach that Vasion Print employs across operating systems.

The app functions as a Vasion Print client and is the receiving agent for centralized print management. It supports printer deployments where printers automatically become available to end users based on specific criteria (e.g., AD/IdP users and groups, IP address ranges, etc.).

When printing directly from the mobile device, jobs are sent directly to the printer using driverless IPP printing. This is included in Vasion Print core functionality.

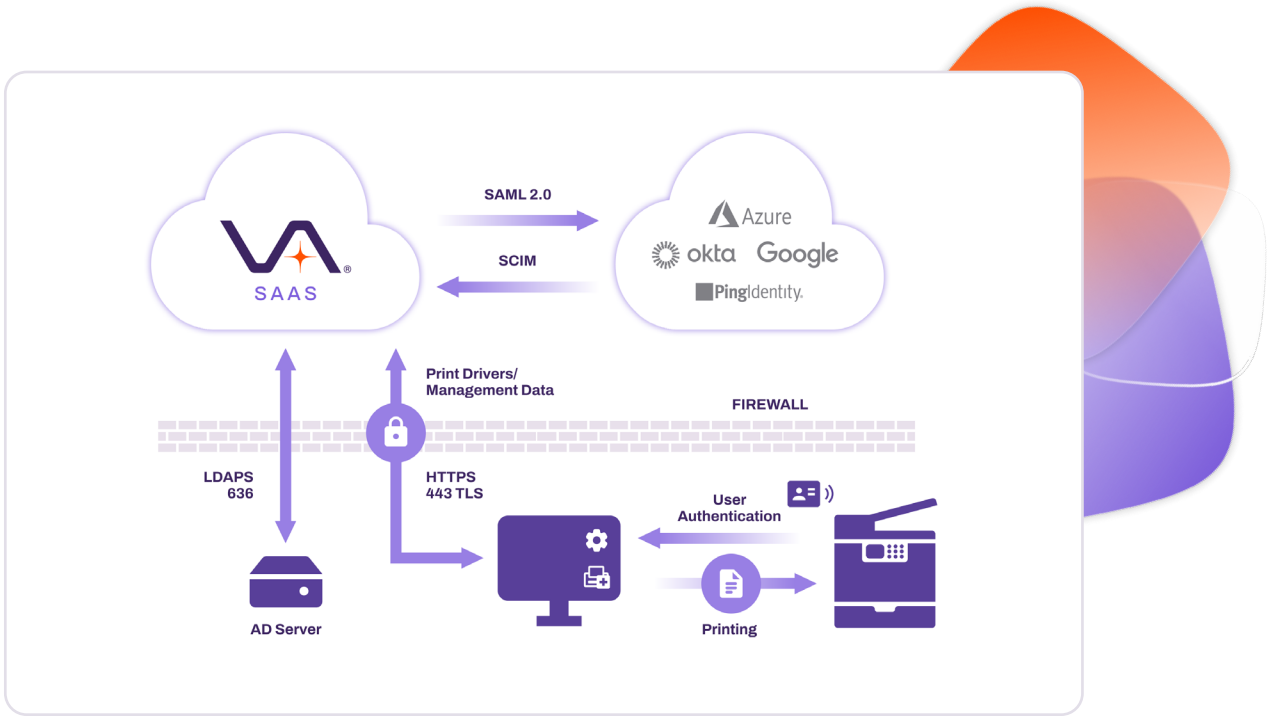

FIGURE 4: Communications flow for Secure Release Printing. Users authenticate against Active Directory, the Vasion Print database, or a cloud-based IdP.

When licensed as part of the Advanced Security Bundle, the Mobile App doubles as a convenient release mechanism for Secure Release Printing, as described in the above section. This bundle also provides Off-Network Mobile Printing and Concurrent (multiple) IdP Support. We explain more about Off-Network Printing below.

Email Printing

Vasion Print offers two Email Printing options: Email Printing and Direct Email Printing. These options use the same configuration, but they handle print jobs differently. These differences are explained below.

- 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 an authenticated user. Emails that pass this test, including attachments, are retrieved from the dedicated mailbox by the Service Client using IMAP port 993 and converted to a PDF. The print job is held on the Service Client until it's released to the target printer via direct IP over port 9100. Email Printing only supports LDAP authentication.

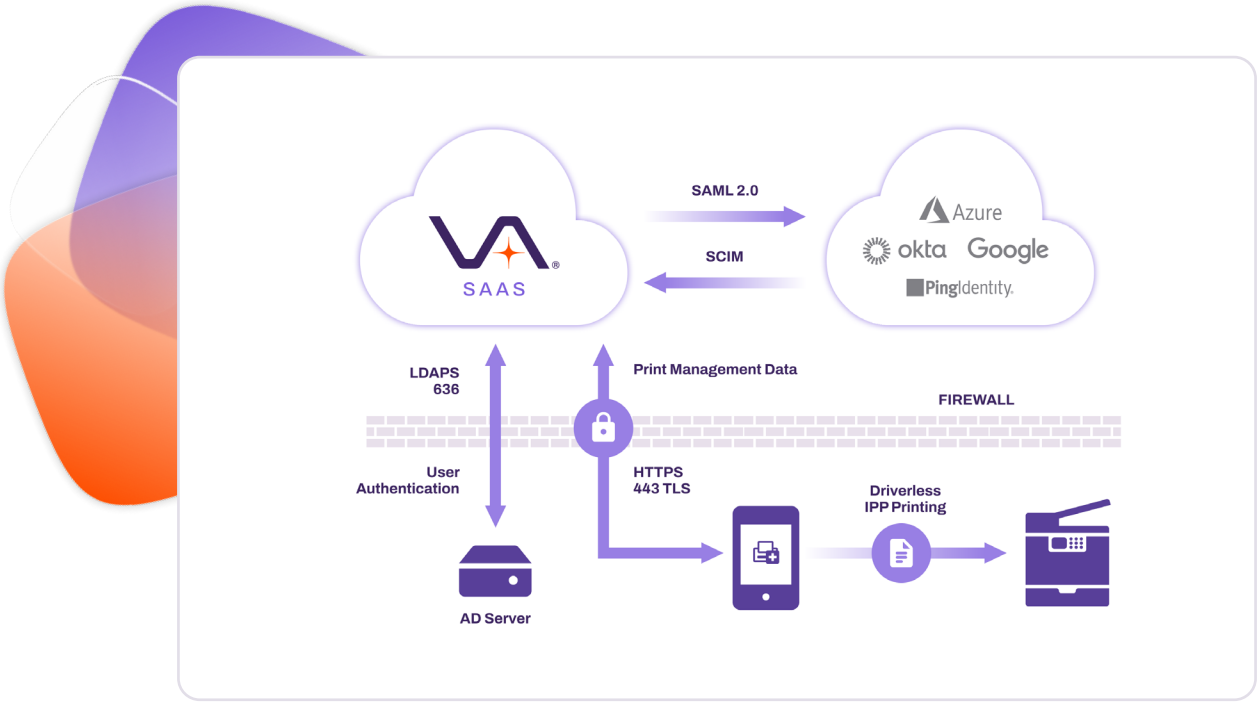

FIGURE 5: Printing directly from the phone uses driverless IPP printing over Port 631 to send the job to the printer.

- With **Direct Email Printing**, the admin creates or specifies a dedicated mailbox using a subdomain that the Vasion Print Service Client monitors. 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 a PDF and sent from the Service Client via direct IP over port 9100 to the target printer. Direct Email Printing only supports LDAP authentication.

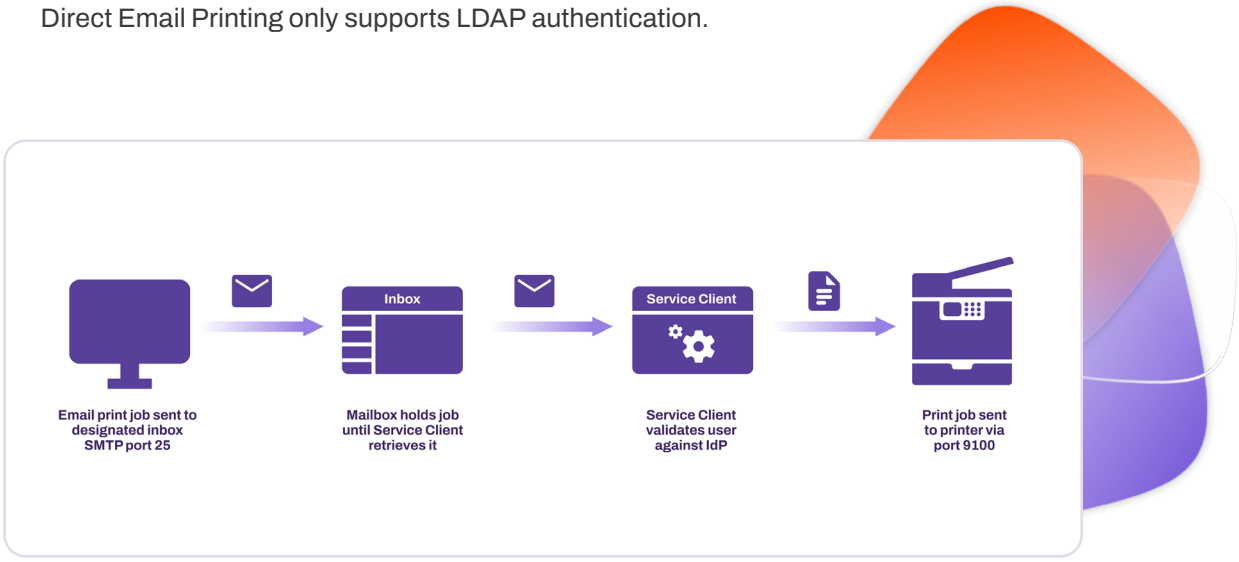

FIGURE 6: Email Printing job flow using a Vasion Print Service Client, including user-identity validation against Active Directory or a cloud-based IdP.

Web Print

For unmanaged users, like guests, Vasion offers Web Print, a secure, easy-to-use solution that offers users the ability to 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 with 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.

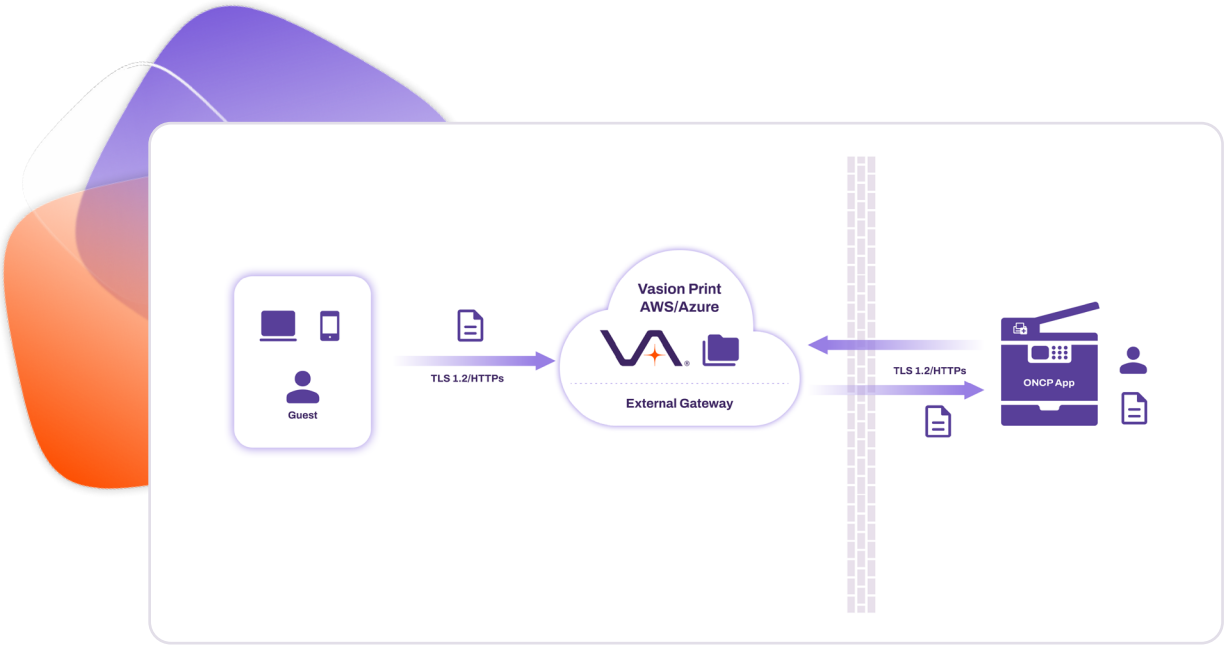

FIGURE 7: Web Print flow for guest users, detailing the process from document upload via a BYOD device to encrypted storage in Vasion's AWS, followed by release confirmation and the ONCP App downloading and printing the document.

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 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.

Off-Network Printing

Many companies employ temporary contractors and remote workers or host their partners, all of whom do not have regular access to the corporate network. Giving them equal open access poses potential security risks to any MFDs residing on the secure network.

All employees, regardless of location, need equal open access to printers behind the company firewall, with internet access, while protecting the network's security. With Off-Network Printing, print traffic is encrypted using TLS 1.2, and any print jobs held on the Service Client for pull or Secure Release will be encrypted while at rest inside the network. Off-Network Printing supports Zero Trust requirements to maintain security, meaning all users must authenticate their identity when printing.

This solution routes print jobs via two main components: the External Gateway and the Internal Routing Service.

- **External Gateway Service:** The External Gateway receives off-network print jobs from remote workstations over HTTPS (port 443) using TLS 1.2 encryption. The External Gateway is hosted as a service in AWS by Vasion Print, with options for self-hosted and hybrid models. If the customer hosts the External Gateway, it will run on a Service Client and requires a Secure Sockets Layer (SSL) certificate.
- **Internal Routing Service:** The Internal Routing Service runs on a Service Client inside the customer's network and watches the External Gateway for incoming print jobs via port 443 using WebSockets. When a print job is sent to the External Gateway, the Internal Routing Service will immediately download it over port 443 and deliver it to the printer over port 9100 or over port 631 for Chromebooks. If the print job is sent using the secure or pull printing feature, it will be held by default on the end user's workstation. The Internal Routing Service can be built with redundancy in the environment.

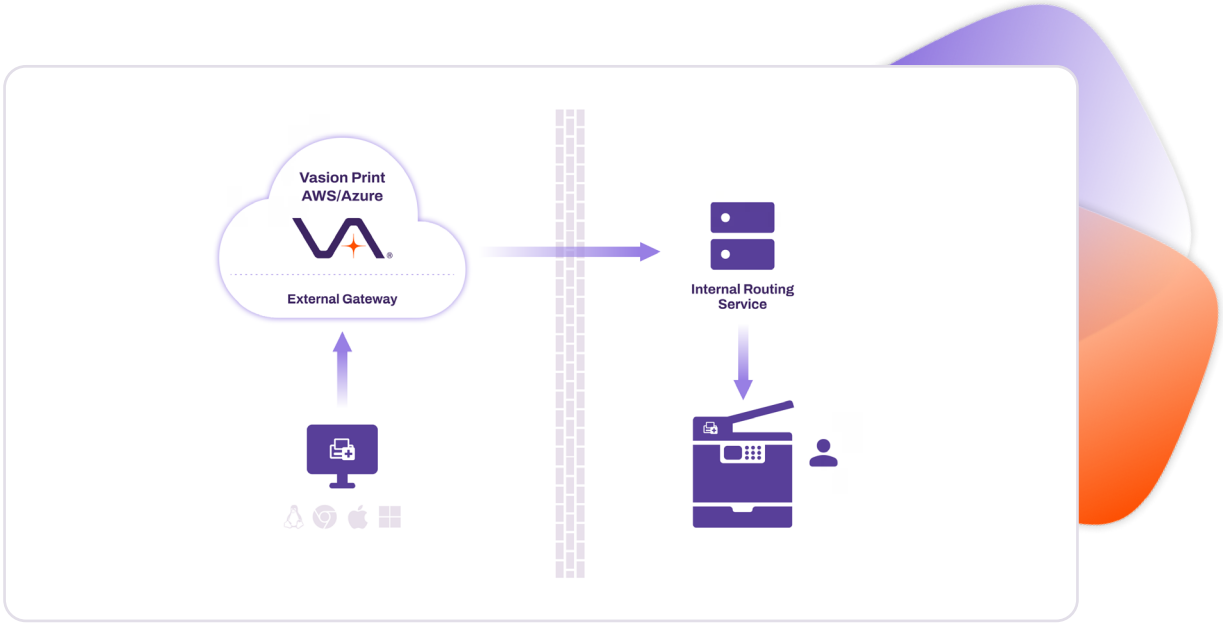

FIGURE 8: With Off-Network Printing, the External Gateway is hosted by Vasion Print in Azure or AWS, and the Internal Routing Service is hosted on-prem by the customer.

Off-Network Mobile Printing

Mobile users often use their mobile carrier's network. They aren't always allowed on the same network where printers reside. Off-Network Printing allows these users to print to a secure printer on the organization's secure network by routing print jobs through the Internal Routing Service Client and sending the job to the printer using direct IP printing. Users authenticate their identity using LDAP or a cloud IdP and then send a print job from the app. The job is encrypted via TLS 1.2 and sent over HTTPS to the External Gateway using port 443. The gateway routes the print job to the Service Client running the Internal Routing Service. Once the printer configured for Off-Network Printing is ready to receive the print job, the Internal Routing Service Client routes it to the printer.

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. This is an advantage because jobs can be released at any time and aren't limited if the workstation that sent the job is offline. The job is not copied or cached and is deleted from the storage when the job is released, ensuring document security while in the cloud.

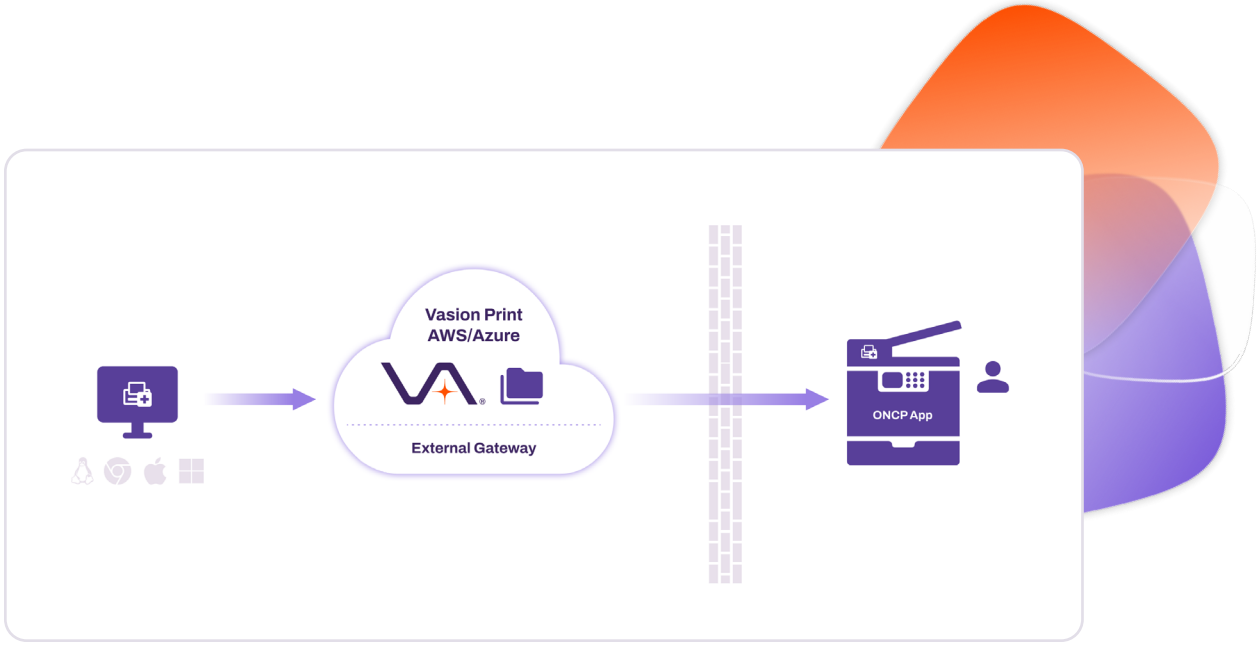

FIGURE 9: Vasion Print's Off-Network Cloud Printing lets users print from anywhere, removing the need for an on-prem Internal Routing Service.

Conclusion

Any SaaS solution that manages the flow and retrieval of confidential information must be secure. With Vasion Print, all communication between workstation clients and the AWS/Azure-hosted Vasion Print instance is encrypted over HTTPS and TLS 443 with an OAuth2 security token. Driver downloads are hash-verified.

Vasion utilizes the security features of Amazon Web Services and Azure Cloud to ensure that Vasion systems and data are secure and take advantage of the AWS ISO 27001-certified platform. In addition, Vasion Print SaaS platform is ISO 27001:2022- and SOC 2 Type 2-certified, underscoring a commitment to protecting your data with optimized, efficient security controls.

With Vasion Print direct IP architecture, every print job stays local, except during Off-Network and Off-Network Cloud Printing. Print job metadata is the only information sent over the WAN to the hosted Vasion Print instance. Vasion Print integrates with one or more IdP services to authenticate and authorize users, groups, and computers. Multi-factor authentication, when provided by the IdP, is available. Confidential data is also protected through a choice of secure pull-printing capabilities.

Vasion Print provides a highly available, secure serverless printing platform that empowers IT administrators to eliminate print servers completely. The SaaS solution converts an existing print environment to centrally managed direct IP printing. It offers printer deployment and management, print auditing and reporting, and centralized printer management from a web-based console. Concerning cost-effectiveness, Vasion has a proven track record for high return on investment. Customers report measurable gains resulting from infrastructure reductions, improved IT efficiencies, optimized printing uptime/reliability, and lower helpdesk costs.

VASION®

Abbreviations Glossary

AES: Advanced Encryption Standard

AD: Active Directory

ADSIs: Active Directory Service Interfaces

AWS: Amazon Web Services

CPA: Control Panel Application

DFS: Distributed File System

EFS: Elastic File System

GPO: Group Policy Object

HTTPS: Hypertext Transfer Protocol Secure

IdP: Identity Provider

IMAP: Internet Message Access Protocol

IPP: Internet Printing Protocol

JIT: Just In Time

LDAP: Lightweight Directory Access Protocol

LDAPS: Lightweight Directory Access Protocol (Over SSL)

MFA: Multi-factor Authentication

NAT: Network Address Translation

OAuth2: Open Authorization 2.0

OIDC: OpenID Connect

ONCP: Off-Network Cloud Printing

ONP: Off-Network Printing

PII: Personally Identifiable Information

SAML 2.0: Security Assertion Markup Language 2.0

SCIM: System for Cross-domain Identity Management

SSL: Secure Sockets Layer

SSO: Single Sign-on

TLS: Transport Layer Security

VPC: Virtual Private Cloud