VASION®

Technischer Überblick: Sicherheit von Vasion-SaaS

Eine operative Zusammenfassung von Sicherheitsdesign und Kommunikationsprotokollen

Inhaltsverzeichnis

Überblick über Vasion und Umfang dieses Whitepapers

Vasion hat sich seinen guten Ruf durch die Bereitstellung einer Druckinfrastruktur ohne Server erarbeitet, die reich an Funktionen, sicher und benutzerfreundlich ist. Die Vasion-Lösung bietet zwei Distributionsmodelle: eine echte SaaS-Implementierung, die die Notwendigkeit von Druckservern, Lizenzen und Wartung überflüssig macht, sowie eine eigenständige Virtual Appliance für den lokalen und Private-Cloud-Einsatz.

Durch die zunehmende Nutzung von Cloud-Lösungen hat sich Vasion Print SaaS als führende Plattform für Neukunden etabliert. Es verwandelt Ihre vorhandene Druckumgebung in ein hoch verfügbares, zentral verwaltetes IP-Direktdruck-System. Für die Bereitstellung und Verwaltung von Druckern und Treibern sind keine Gruppenrichtlinienobjekte (GPOs) oder Skripte erforderlich.

Mit Vasion Print (früher PrinterLogic) werden Druckaufträge von einem Arbeitsplatzrechner (Workstation) direkt über die IP an den Drucker gesendet, sodass alle Druckdaten lokal bleiben, selbst wenn die Funktionen für sicheres Drucken oder Pull-Printing verwendet werden.[1] Druckdaten verlassen das lokale Netzwerk nur bei Verwendung von Off-Network Printing und Off-Network Cloud Printing und werden über HTTPS/SSL verschlüsselt.

Zentrale Komponenten von Vasion Print sind eine Cloud-Instanz (in Amazon Web Services oder Azure Cloud gehostet), eine kleine Anwendung, die auf jeder Workstation installiert wird (ein Client), und der Service-Client.[2] Letzterer bietet zusätzliche Dienste für erweiterte Funktionen, wie sicheres Drucken und Off-Network Printing.

In diesem Whitepaper werden Sicherheits- und betriebsrelevante Details zu Vasion Print SaaS erläutert. Die nachfolgenden Informationen gelten nicht unbedingt für lokale Installationen, auch wenn sich manche Aspekte mit unserer Virtual Appliance überschneiden.

1 Bei der Standardkonfiguration bleiben vertrauliche Daten im lokalen Netzwerk und der WAN-Datenverkehr wird minimiert. Bei manchen erweiterten Konfigurationen, wie nachstehend beschrieben, strömen die Druckdaten auf ihrem Weg zu einem externen Drucker durch Ihre sicheren Cloud-Instanzen.

2 Der Service-Client kann auf Workstations mit Windows, Mac oder Linux installiert werden, die dauerhaft eingeschaltet bleiben.

Die Kommunikation zwischen der Vasion Print-Instanz und dem Client

Vasion ist ein APN Advanced Technology Partner. Unsere SaaS-Lösung erfüllt nach wie vor die Anforderungen gemäß dem AWS-Framework AWS Well-Architected. Hinsichtlich der Hosting-Sicherheit bietet unsere Software sämtliche Vorteile von AWS Cloud Security und Azure Cloud.

Vasion Print nutzt für die Bereitstellung und Verwaltung von Druckern und Standard-Druckeinstellungen ein Instanz-Client-Modell. Der Client ist eine kleine Anwendung, die auf Endbenutzer-Workstations installiert wird. Sie kommuniziert mit der Vasion Print-Instanz über HTTPS mittels Transport Layer Security (TLS 1.2) und einem OAuth2-Sicherheitstoken, das gewährt wird, wenn der Client mit einem gültigen Autorisierungscode installiert wird.

Bei der Anmeldung an der Workstation (sowie in einem geplanten Intervall) verwendet der Workstation-Client das OAuth2-Sicherheitstoken, um Anfragen zu authentifizieren, die an die Vasion Print-Instanz gestellt werden. Der Client sendet über den Port 443 eine HTTPS-Anfrage an die Vasion Print-Instanz, um zu prüfen, ob der Workstation oder dem Benutzer Aktivitäten zugewiesen wurden. Wenn der Workstation-Client über kein gültiges OAuth2-Sicherheitstoken verfügt, wird die Kommunikation mit der Vasion Print-Instanz verweigert und der Benutzer aufgefordert, beim Administrator einen neuen Autorisierungscode anzufordern.

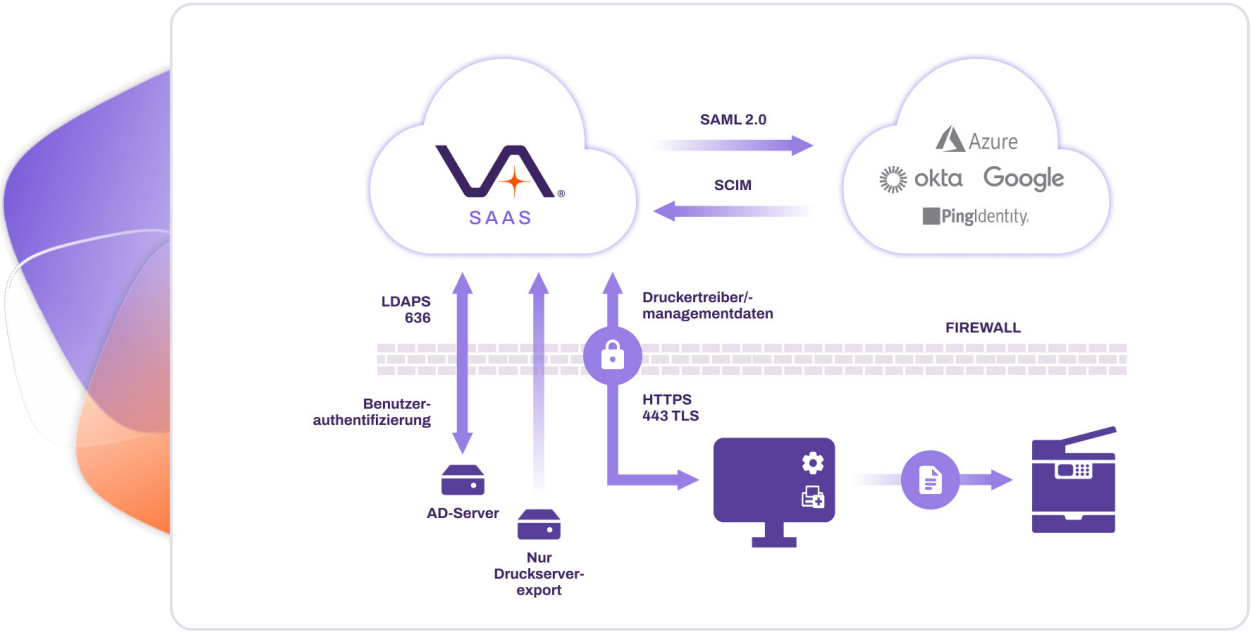

ABBILDUNG 1: Vasion Print-Kommunikationspfade für eine SaaS-Instanz, einen Workstation-Client und Identitätsanbieter (IdPs).

Sobald der Workstation-Client über ein gültiges OAuth2-Sicherheitstoken verfügt, wird sämtliche Kommunikation (wie Installation und Updates von Treibern und Profilen, Client-Updates, Metadaten-Berichte und Client-Anmeldungen) über TLS 1.2 verschlüsselt.

Den Autorisierungscodes für OAuth2-Sicherheitstoken werden Ablauffristen zugewiesen. Werden die Autorisierungscodes nicht innerhalb der zugewiesenen Frist verwendet, werden sie ungültig und ein neuer muss generiert werden. Falls nötig, kann der Administrator ein OAuth2-Sicherheitstoken für jede Workstation widerrufen. In diesem Fall fordert der Workstation-Client einen neuen Autorisierungscode an. Sobald der neue Code eingegeben wurde, wird dem Client ein neues OAuth2-Sicherheitstoken gewährt.

Die Vasion Print Admin Console und die Bereitstellung von Treibern

Druckertreiber können manuell auf die Vasion Print-Instanz hochgeladen werden. Vasion Print bietet auch ein Druckserver-Importtool, das Treiber und Profile automatisch von einem oder mehreren Druckservern importieren kann, die später außer Betrieb genommen werden.

Die Vasion Print Admin Console identifiziert spezifische Druckertreiber, die vom Workstation-Client installiert werden müssen.[3] Wenn sich ein Client anmeldet und die Liste der zu installierenden Treiber erhält, überprüft er zunächst, ob der Treiber bereits auf der lokalen Workstation vorhanden ist. Ist dieser nicht verfügbar, lädt der Client den Treiber von der Vasion Print-Instanz oder einem speziellen Treiber-Cache herunter. Der Treiber wird dann mithilfe von System-Service-Privilegien auf der Workstation installiert. Nur Treiber, die ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle (in der Regel der Druckerhersteller) haben, werden von Vasion Print installiert. Der Workstation-Client konfiguriert den Treiber gemäß den Profileinstellungen, die in der Admin Console festgelegt sind.

Wenn Druckertreiber von der Vasion Print-Instanz heruntergeladen werden, werden sie über einen verschlüsselten Port (443) mittels TLS 1.2 gesendet und mit einer Hash-Prüfung bestätigt. Treiber können auch in einem lokalen Cache über ein verteiltes Dateisystem (Distributed File System, DFS), eine Dateifreigabe oder eine permanent verfügbare Workstation gespeichert werden. Workstations können dann die Treiber vom lokalen Cache abrufen, anstatt sie von der Vasion Print-Instanz herunterladen zu müssen. Druckertreiber werden über Port 443 von der Vasion Print-Instanz heruntergeladen, obfuskiert und in der Dateifreigabe gespeichert. Andere Workstation-Clients in der Umgebung rufen Druckertreiber von der Dateifreigabe über Port 445 ab – eine Standardkommunikationsmethode in einem auf Microsoft basierenden LAN.

Direkte IP-Druckaufträge bleiben im lokalen Netzwerk

Druckaufträge werden von Windows-, Mac- und Linux-Workstations über direkte IP unmittelbar zum Drucker gesendet, und zwar standardmäßig über Port 9100 oder wie es in der Vasion Print-Instanz hinterlegt ist. Die Erweiterung für den **ChromeOS-Client** und die Mobil-App (iOS und Android) senden Druckaufträge über IPP über Port 631.[4]

Für Berichtszwecke werden Metadaten und grundlegende personenbezogene Daten wie Benutzername, E-Mail-, IP-Adresse und Computername für Druckaufträge per TLS 1.2 an die Vasion Print-Instanz gesendet, darunter Metadaten wie Datum und Uhrzeit des Druckauftrags, Benutzer, Ursprungs-Workstation, Druckername, Dokumententitel, Seitenformat und Seitenzahl. Die Übertragung des Dokumententitels kann in der Admin Console deaktiviert werden.

In manchen Fällen kann es vorkommen, dass eine Workstation oder ein Mobilgerät keine IP-Verbindung zum Drucker hat. Hier können die Vasion-Funktionen Off-Network Printing und Off-Network Cloud Printing helfen, Druckaufträge sicher über Zero-Trust-Netzwerkgrenzen hinaus zu übertragen. Näheres dazu erfahren Sie im Abschnitt „Off-Network Printing“.

3 Die Ausnahme ist die ChromeOS-Erweiterung, die die treiberlose Internet-Printing-Protocol-Technologie (IPP) verwendet.

4 Aufgrund von Sicherheitslimits des Betriebssystems verwenden ChromeOS-Geräte die Vasion Print-Erweiterung für ChromeOS anstelle des Vasion Print-Clients. Sie bietet ähnliche Funktionen, kann aber nicht zum Service-Client gemacht werden.

Kommunikation mit Microsoft Active Directory

Vasion Print kann einen oder mehrere Identitätsanbieter-Dienste (IdP) wie die Legacy-Active-Directory-Unterstützung nutzen, um Benutzer, Gruppen und Workstations für verschiedene optionale Funktionen zu authentifizieren und zu autorisieren. Dazu zählt auch die Authentifizierung für die Admin Console, Pull-Printing und mobiles Drucken.

Zur Konfiguration von Vasion Print für die Integration mit Active Directory (AD) sind mehrere Schritte erforderlich. Da sich die Vasion Print-Instanz außerhalb der Firewall befindet, muss der IT-Administrator sicherstellen, dass die Firewall-Regeln den Zugriff auf das Active Directory über den verschlüsselten LDAPS-Protokollport (636) erlauben.

Wenn Vasion Print mit dem AD-Server kommuniziert, wird die Kommunikation von der Vasion Print-Instanz innerhalb der Vasion Print Virtual Private Cloud (VPC) über ein NAT-Gateway initiiert. So kann der Kunde die Firewall-Regel auf eine einzelne statische Quell-IP-Adresse beschränken, die auf der geografischen Region der Vasion Print-Instanz basiert. Die LDAPS-Anfrage wird per TLS 1.2 bis zur Firewall des Kunden verschlüsselt, die die Anfrage dann direkt zum LDAPS-Endgerät weiterleitet.

Die Vasion Print-Instanz hat beim Zugriff auf den AD-Server lediglich Lesezugriff. Jedes Mal, wenn ein Authentifizierungsversuch oder die Prüfung der Mitgliedschaft in einer AD-Gruppe erforderlich ist (z. B. E-Mail-Druck, Authentifizierung bei der Control Panel Application über AD-Benutzername und Passwort), kontaktiert Vasion Print AD über ein BIND-Servicekonto. Die Informationen des BIND-Kontos werden verschlüsselt und in der Vasion Print-Datenbank gespeichert. Für zusätzliche Sicherheit kann der Administrator ein BIND-Servicekonto mit Lesezugriff verwenden.[5]

Einige Vasion-Funktionen wie E-Mail-Druck und sicheres Drucken mit der Vasion Print Control Panel Application erfordern die LDAP-Synchronisierungsfunktion, die über die Identitätssynchronisierungs-Registerkarte im Service-Client aktiviert wird. Die LDAP-Synchronisierungsfunktion synchronisiert bestimmte Attribute wie AD-Benutzernamen, Ausweis-IDs, PIN-Codes und E-Mail-Adressen und speichert sie im Benutzer-Mikrodienst von Vasion Print. Diese Daten werden lokal von der LDAP-Synchronisierungsfunktion mithilfe des BIND-Kontos abgerufen und über Port 443 per TLS 1.2 in die Vasion Print-Instanz hochgeladen.

Der auf der Endbenutzer-Workstation installierte Client stellt zur Benutzerauthentifizierung keine direkte Verbindung zur Vasion Print-Instanz her. Stattdessen führt der Client von einer Windows-Workstation aus eine Authentifizierung bei Active Directory über Active Directory Service Interfaces (ADSIs) durch. Bei Mac- oder Linux-Workstations verwendet er Kerberos-Tickets.

5 Eine alternative Methode für die LDAP-Authentifizierung ist die LDAP-Identitätssynchronisierung. Durch Konfiguration des LDAP-Identitätssynchronisierungsservices auf einem Service-Client werden LDAP-Queries hinter der Firewall gehalten und über HTTPS an Vasion übermittelt. Die Active Directory-Passwörter der Benutzer werden nicht in LDAP gespeichert und niemals mit Ihrer Vasion-Instanz synchronisiert.

Kommunikation mit cloudbasierten Identitätsanbietern (IdPs)

Aktuell unterstützt Vasion folgende IdPs:

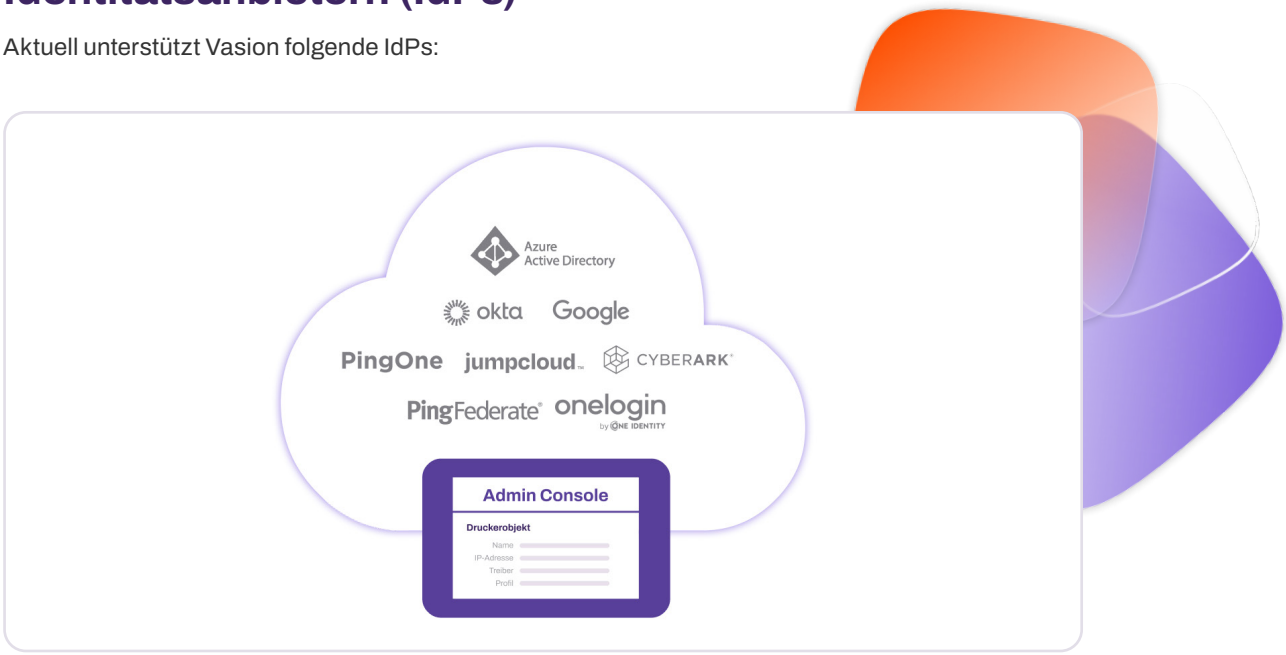

ABBILDUNG 2: Derzeit unterstützt Vasion die oben angegebenen Identitätsanbieter und kann auf Anfrage weitere IdPs hinzufügen.

Wenn Vasion Print für die Integration mit einem cloudbasierten Identitätsanbieter wie Okta oder Azure AD konfiguriert wurde, werden die in der IdP-Konsole verwalteten Benutzerinformationen mit Vasion Print synchronisiert. Dies erfolgt entweder über das System for Cross-domain Identity Management (SCIM) oder Just-in-Time-Bereitstellung (JIT), wenn sich ein Benutzer zum ersten Mal anmeldet.

Wenn der cloudbasierte IdP keine native SCIM-Unterstützung bietet, hat Vasion Print einen ähnlichen Service, der auf einem Service-Client läuft und die IdP-Benutzer und -Gruppen synchronisiert. Die Synchronisierung zwischen dem IdP und Vasion Print kann bei Okta nahezu sofort erfolgen und bei Azure AD bis zu 40 Minuten dauern.

Zusätzlich erfolgt die Anmeldung an der Vasion Print-Instanz über den IdP mittels Security Assertion Markup Language 2.0 (SAML 2.0) oder OpenID Connect (OIDC) bei Google. Die vom IdP bereitgestellten synchronisierten Identitätsinformationen werden zur Autorisierung folgender Vorgänge verwendet:

- Zugriff auf das Self-Service-Installationsportal von Vasion Print
- Zugriff auf die Vasion Print Admin Console
- Authentifizierung für die Freigabe von Druckaufträgen
- Vasion Print-Client mit dem IdP-Benutzer
- Druckerbereitstellungen

Erweiterte Sicherheitsfunktionen wie Mehrfaktor-Authentifizierung (MFA) und Single Sign-on (SSO), sofern aktiviert, werden vom Identitätsanbieter verwaltet. Diese Funktionen verbessern die Authentifizierungssicherheit und bieten Produktivitätsvorteile für Endbenutzer.

Weitere Informationen dazu, wie sich Vasion Print mit führenden IdPs integrieren lässt, sowie Betriebsdetails und Sicherheitsstandards finden Sie **in diesem Whitepaper**.

Vasion Print-Service-Client

Funktionsüberblick

Der Vasion Print-Service-Client ermöglicht erweiterte Funktionen der serverlosen Plattform von Vasion Print. Er ermöglicht die Kommunikation zwischen der Vasion Print-Instanz und erweiterten Vasion Print-Funktionen und sorgt dafür, dass vertrauliche Druckdaten bei Standardkonfiguration im lokalen Netzwerk bleiben.

Folgende Funktionen benötigen den Service-Client:

- Off-Network Printing
- Installation der Control Panel Application (CPA) auf Druckern
- Authentifizierung an der Control Panel Application (Freigabe per Ausweis, Benutzer-ID/PIN)
- Einfache Freigabe per Ausweis (für Netzwerkdrucker ohne Konsolenschnittstelle)
- SNMP-Überwachung (wenn die Service-Client-Option aktiviert ist)
- E-Mail-Druck (Standard, direkt)
- Identitätssynchronisierungsservice (für IdPs ohne native SCIM-Unterstützung)
- Sichere Offline-Freigabe für Windows-Endgeräte

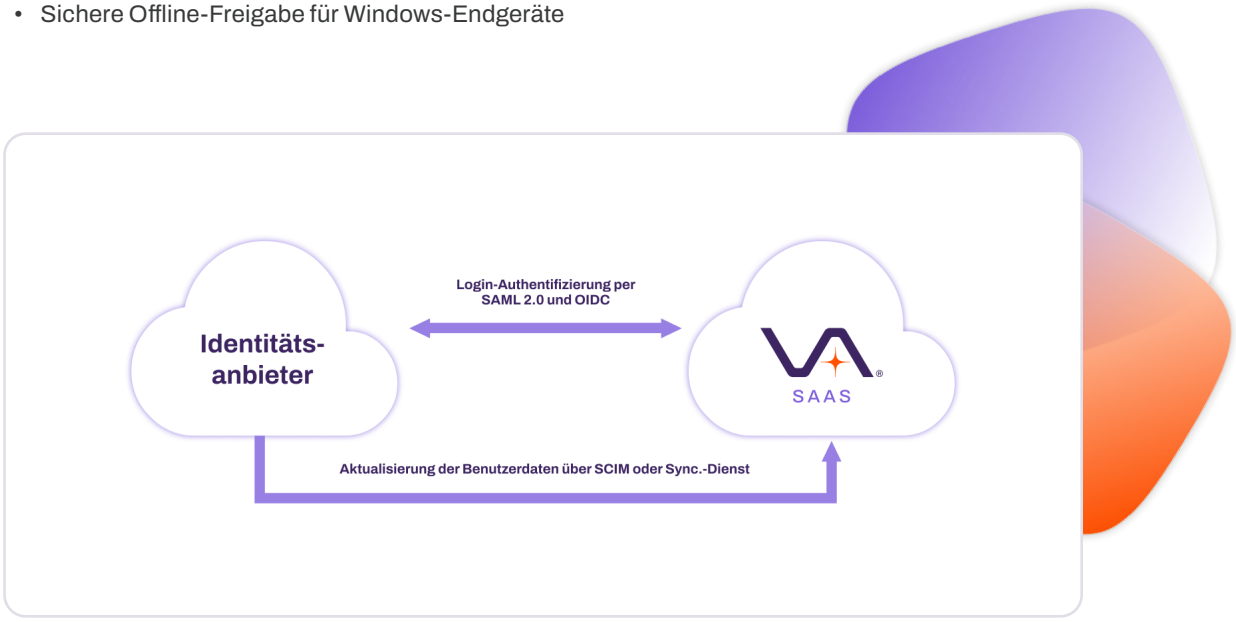

ABBILDUNG 3: SCIM, OIDC und SAML 2.0 in der Vasion Print-Integration.

So wird der Service-Client konfiguriert

Die Konfiguration eines Service-Clients erfolgt in drei Schritten. Zunächst wird mithilfe des Hostnamens oder der IP-Adresse einer Windows-, Mac- oder Linux-Workstation, die dauerhaft eingeschaltet bleibt, ein Service-Client-Objekt im Navigationsbaum der Admin Console erstellt. Dann wird der Vasion Print-Client auf dieser Workstation gemäß dem im Abschnitt *Die Kommunikation zwischen der Vasion Print-Instanz und dem Client* beschriebenen Sicherheitsprozess installiert. Wenn sich der Client dann an der Vasion Print-Instanz anmeldet, erkennt er, dass er zum Service-Client konfiguriert wurde, und startet die Prozesse für die aktivierten erweiterten Funktionen. Das OAuth2-Sicherheitstoken des Clients wird verwendet, um ein zweites OAuth2-Sicherheitstoken von der Vasion Print-Instanz anzufordern.

Hier ist eine Liste der verfügbaren Service-Client-Prozesse:

• Off-Network Printing	PrinterLogicServiceOffNetworkServer
• Off-Network Printing	PrinterLogicServiceOffNetworkClient
• Control Panel App	PrinterLogicServicePrinterApp
• Einfache Freigabe per Ausweis	PrinterLogicServiceSimpleBadgeRelease
• SNMP-Überwachung	PrinterLogicServiceSNMP
• E-Mail-Druck	PrinterLogicServiceEmail
• Identitätssynchronisierungsservice	PrinterLogicServiceIdentitySync
• Sichere Offline-Freigabe	PrinterLogicServiceOfflinePrint

Methoden für sicheres Drucken

Vasion bietet drei sichere Druckmethoden:

- Pull-Printing (eine virtuelle Druckerwarteschlange, bei der der Benutzer später entscheidet, wo er den Druckauftrag abholt)
- Sicheres Drucken (ein spezifischer Drucker wird so konfiguriert, dass er vertrauliche Druckaufträge empfangen kann)
- Sicheres Offline-Drucken (ein Druckauftrag wird initiiert, die Ursprungs-Workstation geht offline, der Ausdruck erfolgt später)

Beim **Pull-Printing**-Szenario druckt der Benutzer auf einem sicheren virtuellen Pull-Drucker, der den Druckauftrag auf der Workstation des Benutzers zurückhält, bis sich der Benutzer am Drucker seiner Wahl authentifiziert und den Ausdruck entnehmen kann.

Beim Szenario mit **sicherem Drucken** weist der Administrator einen physischen Drucker als sicheres Gerät aus. Wenn ein Benutzer auf einem dieser Drucker ausdruckt, muss er über eine Eingabeaufforderung angeben, ob der Druckauftrag zurückgehalten oder sofort freigegeben werden soll. Die Eingabeaufforderung ist optional. Drucker können so konfiguriert werden, dass Druckaufträge immer zurückgehalten oder immer sofort freigegeben werden. Wenn Druckaufträge immer zurückgehalten werden sollen, müssen Benutzer sich am ausgewiesenen Drucker authentifizieren, um den Druckauftrag freigeben zu können.

Bei beiden Optionen wird der Druckauftrag vom Druckertreiber gerendert und in einem Roh- oder binären Format auf der Workstation des Benutzers unter dem Pfad C:\Windows\System32\spool\PRINTERS\held\local gespeichert. Dies ist ein sicherer Ordner, auf den nur Administratoren zugreifen können, bis der Benutzer den Druckauftrag am Drucker freigibt.

Beim **sicheren Offline-Drucken** initiiert der Benutzer den Druckauftrag und hat dann die Option, seinen Laptop oder Rechner herunterzufahren und den Druckauftrag später zu empfangen. Zunächst wird eine Kopie des Druckauftrags auf der Workstation zurückgehalten. Darüber hinaus wird eine Kopie des Druckauftrags im Rohformat an den Vasion Print-Service-Client über Port 31989 gesendet, wo sie mit einem OpenSSL-AES-256-Algorithmus verschlüsselt wird. Im gespeicherten Zustand verbleibt sie verschlüsselt auf dem Service-Client im Ordner C:\Program Files (x86)\Printer Properties Pro\Printer Installer Client\service-offline-print\jobs\held.

Wenn der Endbenutzer zu einem Drucker geht, um den Druckauftrag freizugeben, versucht Vasion zunächst, den Auftrag freizugeben, der auf der Workstation gespeichert ist. Ist die Workstation offline, kontaktiert Vasion den Service-Client, um die verschlüsselte Kopie freizugeben. Bei letzterem Szenario wird der Druckauftrag über OpenSSL auf dem Service-Client verschlüsselt und an den Zieldrucker gesendet.

Sobald der sichere Druckauftrag freigegeben wurde, wird die Extrakopie entweder von der Workstation des Benutzers (sobald der Computer wieder online ist) oder vom Service-Client gelöscht, je nachdem, wie der Auftrag ausgeführt wurde.

Sicheres Offline-Drucken in einem lokalen Netzwerk wird für Windows-Endgeräte unterstützt. Off-Network Cloud Printing ermöglicht das sichere Offline-Drucken, bei dem sich die Ursprungs-Workstation in einem anderen Netzwerk befindet als der Zieldrucker. Dies ist besonders für Zero-Trust-Umgebungen nützlich.

Authentifizierungsmethoden für die sichere Freigabe

Vasion Print SaaS unterstützt fünf Mechanismen für die sichere Freigabe und Pull-Druckaufträge:

1. **Freigabe per Smartphone mit QR-Code:** Unsere Mobil-App ist im Google Play Store oder Apple App Store erhältlich. Nach der Installation geben die Benutzer die URL ihrer Vasion Print-Instanz sowie die Anmeldedaten für Active Directory oder den IdP ein. Sobald die Authentifizierung abgeschlossen ist, werden verfügbare sichere und Pull-Druckaufträge auf ihrem Bildschirm angezeigt. Die Kommunikation zwischen der App und der Vasion Print-Instanz erfolgt über HTTPS und den Port 443.

   Beim Pull-Printing können Benutzer einen QR-Code auf einem Drucker in der Nähe scannen, um das gewünschte Ausgabegerät zu identifizieren. Verwendet der Benutzer die App zur Freigabe des Druckauftrags, weist Vasion Print den Workstation-Client des Benutzers über Port 443 an, den Auftrag auszudrucken. QR-Codes funktionieren mit allen Druckern und bieten Benutzern eine bequeme, schnelle Möglichkeit, Drucker zu identifizieren, ohne dessen Namen zu kennen.

2. **Control Panel Application (CPA):** Sobald die Vasion Print CPA auf einem kompatiblen Netzwerkdrucker installiert wurde, können sich Benutzer mit ihren AD-Zugangsdaten, der Benutzer-ID und einem PIN-Code oder einem Freigabecode aus einer E-Mail am Drucker anmelden. Ihnen werden alle zurückgehaltenen Druckaufträge angezeigt, die sich in der Pull-Printing-Warteschlange befinden, sowie alle Druckaufträge, die speziell an diesen Drucker zur sicheren Freigabe gesendet wurden. Werden die AD-Zugangsdaten für die Authentifizierung verwendet, werden sie obfuskiert und über Port 443 verschlüsselt an die Vasion Print-Instanz und über Port 636 an den AD-Server gesendet. Die IdP-Authentifizierung in der CPA unterstützt derzeit PIN-Code und Ausweis, aber nicht Benutzername und Passwort.

3. **Control Panel Application (CPA) mit Ausweis-/Kartenleser:** Wenn ein unterstützter Drucker über einen integrierten Ausweisleser verfügt – oder ein optionaler Ausweisleser angeschlossen ist – können Benutzer ihren Ausweis für die automatische Authentifizierung einlesen. Ausweise und PINs können über eine aktive LDAP-Verbindung oder der LDAP-Synchronisierungsfunktion von Vasion Print erfasst werden. Damit ist keine Firewall-Regel mehr erforderlich. Die Ausweis-IDs von Endbenutzern werden mit dem CPA-Ausweisregistrierungsprozess oder einem vom Systemadministrator festgelegten Attribut in der Vasion Print-Datenbank gespeichert. Beim Lesen des Ausweises wird die Ausweis-ID mit den IDs abgeglichen, die in der Vasion Print-Datenbank (über Port 443) oder in Active Directory (über Port 636) gespeichert sind. Nach der Authentifizierung kann der Benutzer einen einzelnen Druckauftrag oder alle zurückgehaltenen Druckaufträge auf diesem Drucker freigeben.

4. **Einfache Freigabe per Ausweis:** Durch die Verbindung eines Netzwerkgeräts ELATEC TCPConv 2 oder rf IDEAS® E-241 und eines kompatiblen Ausweislesers mit einem Netzwerkdrucker kann der Drucker für eine schnelle, einfache Freigabe zurückgehaltener Druckaufträge verwendet werden. Wenn der Benutzer seinen Ausweis am Leser präsentiert, wird die Ausweis-ID über Port 31990 an den Vasion Print-Service-Client gesendet. Der Service-Client leitet diese Informationen dann über Port 443 an die Vasion Print-Instanz weiter, wo die ID einem registrierten Benutzerkonto zugeordnet wird. Vasion Print autorisiert den Benutzer und sendet über Port 443 einen Freigabebefehl an das ELATEC oder das rf IDEAS®-Gerät und dann werden die Druckaufträge des Benutzers freigegeben.

   Der Administrator kann die einfache Freigabe per Ausweis so konfigurieren, dass entweder der neueste oder alle zurückgehaltenen Druckaufträge in einem Schritt ausgedruckt werden. Die Funktion ist mit den meisten Druckermodellen kompatibel, erfordert aber den Kauf von Ausweislesegeräten. Manche Administratoren bevorzugen die Freigabe per Smartphone mit QR-Code, um zusätzliche Hardwarekosten zu vermeiden.

5. **Webbasiertes Freigabeportal:** Benutzer können sich mit ihren AD- oder IdP-Zugangsdaten über jedes internetfähige Gerät (z. B. Smartphone, Laptop oder PC) am Vasion Print-Freigabeportal anmelden. Das Portal zeigt die zurückgehaltenen Druckaufträge an und ermöglicht die Freigabe auf einem oder mehreren designierten sicheren Druckern. Alternativ können sie über dieselbe Schnittstelle einen Zieldrucker auswählen. Das Freigabeportal authentifiziert den Benutzer über den LDAPS-Port 636 mit dem Active-Directory-Server. Bei Verwendung eines IdPs werden Benutzer zur Authentifizierung an das IdP-Portal weitergeleitet, wo sie ihre Zugangsdaten zur Überprüfung eingeben müssen.

Direkter IP-Druck für Mobilgeräte

Mobilgeräte sind allgegenwärtig und je nach den Anforderungen an die Rechenleistung sind sie mittlerweile zur Workstation der Wahl für einige Benutzer und Umgebungen geworden. In der Vergangenheit war für das Drucken über Mobilgeräte oft ein Drucker mit Spezialfunktionen, Cloud-Druckdiensten oder Konfigurationen erforderlich, die sich nicht wie andere Endgeräte verwalten ließen.

Die Mobil-App für iOS und Android behandelt das Mobilgerät wie jedes andere Endgerät. Mit der App können Benutzer *nativ drucken*, und zwar über denselben Direkt-IP-Ansatz, den Vasion Print betriebssystemübergreifend anwendet.

Die App fungiert als Vasion Print-Client und empfangender Agent für das zentralisierte Druckmanagement. Sie unterstützt Druckerbereitstellungen, wo Drucker Benutzern anhand bestimmter Kriterien (z. B. AD-/IdP-Benutzer und -Gruppen, IP-Adressbereiche usw.) automatisch zur Verfügung gestellt werden.

Beim direkten Druck über das Mobilgerät werden Druckaufträge mittels treiberlosen IPP-Drucks direkt an den Drucker gesendet. Dies ist in der Kernfunktionalität von Vasion Print enthalten.

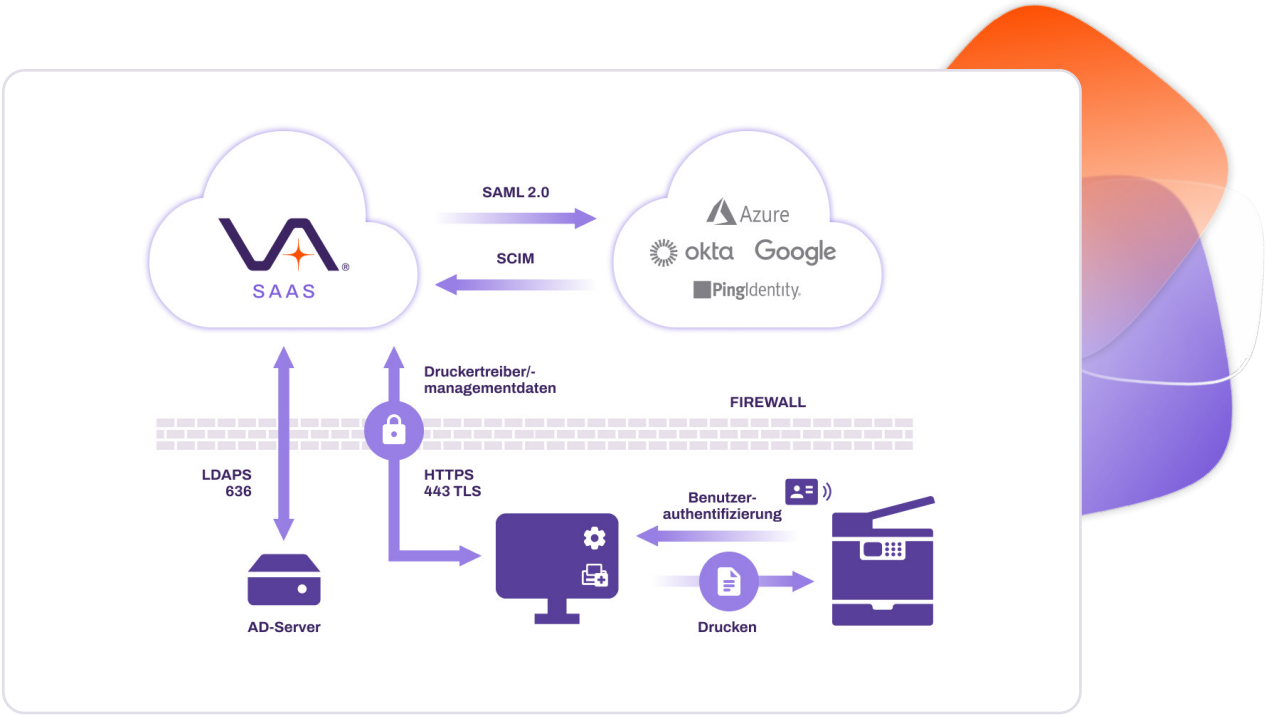

ABBILDUNG 4: Kommunikationsfluss für sicheres Drucken. Benutzer authentifizieren sich bei Active Directory, der Vasion Print-Datenbank oder einem cloudbasierten IdP.

Wenn es als Teil des Advanced Security Bundles lizenziert ist, agiert die Mobil-App gleichzeitig als praktischer Freigabemechanismus für sicheres Drucken, wie im Abschnitt oben beschrieben. Dieses Bundle bietet auch Off-Network Printing für Mobilgeräte und Unterstützung für mehrere IdPs gleichzeitig. Näheres zu Off-Network Printing erläutern wir unten.

E-Mail-Druck

Vasion Print bietet zwei E-Mail-Druck-Optionen: E-Mail-Druck und direkter E-Mail-Druck. Diese Optionen verwenden dieselbe Konfiguration, führen die Druckaufträge aber unterschiedlich aus. Diese Unterschiede werden nachstehend erklärt.

- Beim **E-Mail-Druck** erstellt oder legt der Administrator ein bestimmtes Postfach fest, das der Vasion Print-Service-Client überwacht. Jede E-Mail, die an dieses Postfach gesendet wird, wird mit einem BIND-Konto mit AD abgeglichen, um zu überprüfen, ob der Absender ein authentifizierter Benutzer ist. E-Mails, einschließlich Anhängen, die diese Prüfung bestehen, werden vom Service-Client über IMAP und Port 993 von dem festgelegten Postfach abgerufen und in ein PDF-Dokument konvertiert. Der Druckauftrag wird auf dem Service-Client zurückgehalten, bis er auf dem Zieldrucker über direkte IP über Port 9100 freigegeben wird. Der E-Mail-Druck unterstützt nur die LDAP-Authentifizierung.

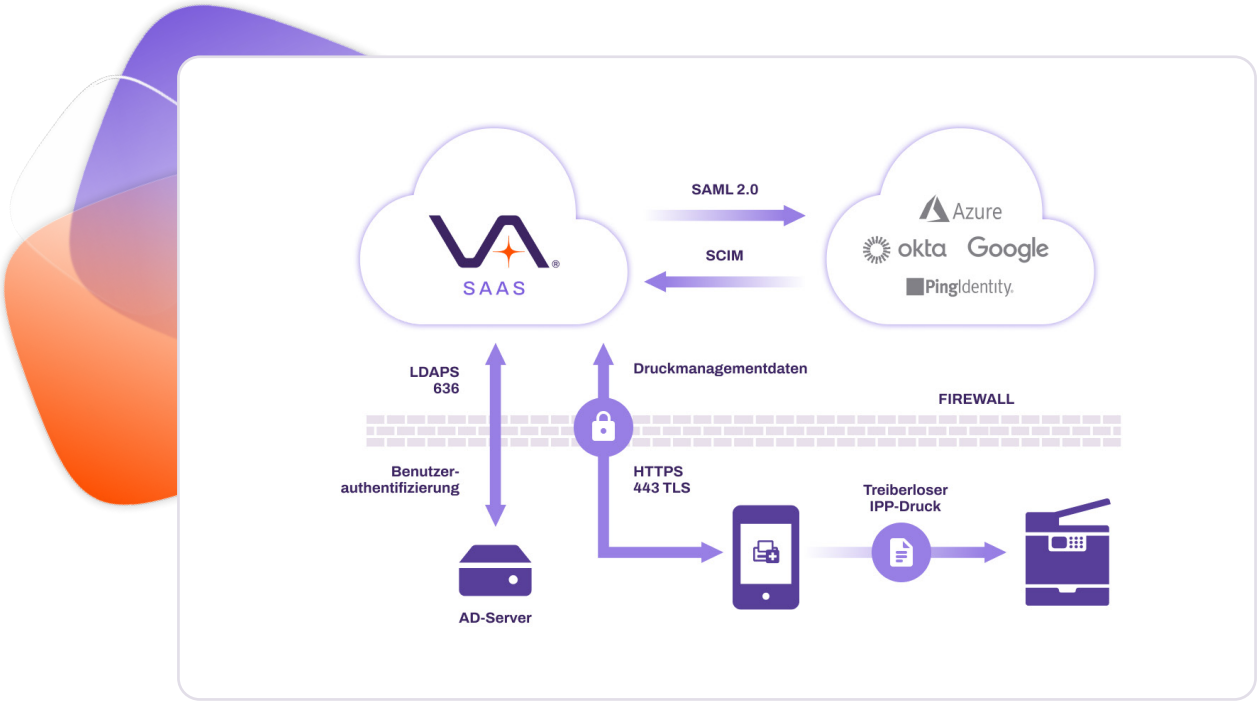

ABBILDUNG 5: Direkter Druck vom Smartphone mithilfe von treiberlosem IPP-Drucken über Port 631, um den Druckauftrag an den Drucker zu senden.

- Beim **direkten E-Mail-Druck** erstellt oder legt der Administrator mit einer Subdomäne ein bestimmtes Postfach fest, das der Vasion Print-Service-Client überwacht. Eine E-Mail-Weiterleitungsregel wird innerhalb des E-Mail-Serviceanbieters erstellt, um E-Mails, die an das Subdomänen-Postfach gesendet wurden, an das primäre E-Mail-Druck-Postfach weiterzuleiten. Jede E-Mail, die unmittelbar an die E-Mail-Adresse für den direkten E-Mail-Druck gesendet wird, wird vom Service-Client abgerufen und mittels eines BIND-Kontos mit AD abgeglichen, um zu überprüfen, ob der Absender ein authentifizierter Benutzer ist. Sie wird auch mit der E-Mail-Adresse des Zieldruckers abgeglichen, die in der Vasion Print Admin Console zugeordnet ist. Alle E-Mails, einschließlich Anhängen, die diese Prüfung bestehen, werden in PDF-Dokumente konvertiert und vom Service-Client über direkte IP und Port 9100 zum Zieldrucker gesendet. Der direkte E-Mail-Druck unterstützt nur die LDAP-Authentifizierung.

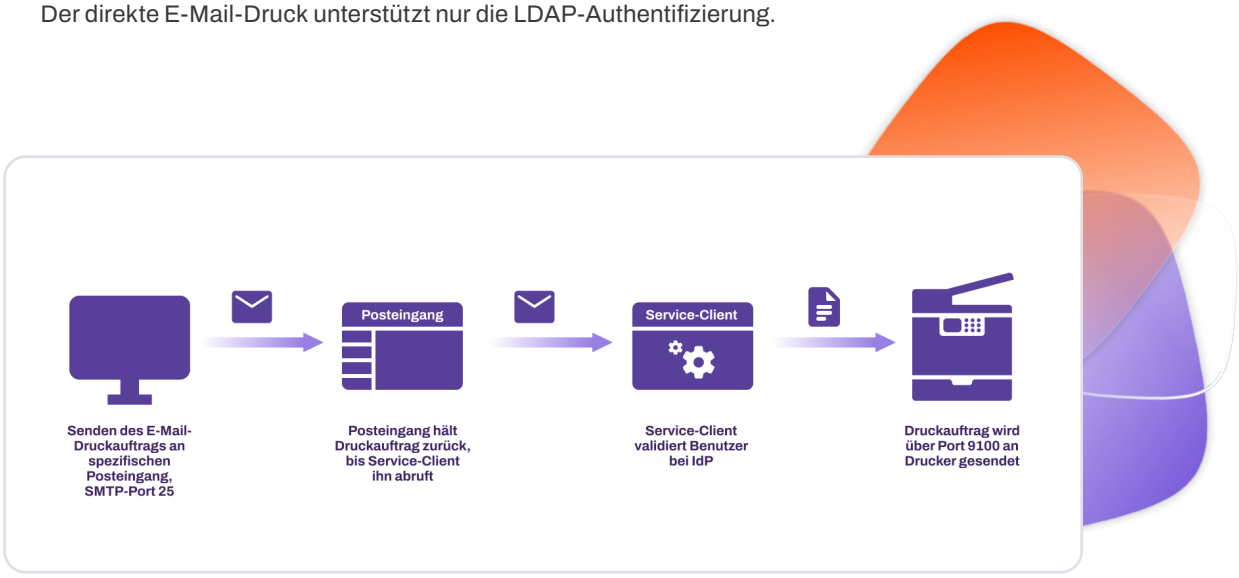

ABBILDUNG 6: Weg eines Druckauftrags beim E-Mail-Druck über einen Vasion Print-Service-Client, einschließlich Überprüfung der Benutzeridentität bei Active Directory oder einem cloudbasierten IdP.

Web-Druck

Mit dem Web-Druck von Vasion können nicht verwaltete Benutzer wie Gäste bequem und sicher über einen Web-Browser drucken, ohne dass zusätzliche Software oder Zugriff auf Ihr Netzwerk erforderlich ist. Wenn der Web-Druck aktiviert ist, sendet Vasion eine individuelle URL zu einem Web-Portal. Unternehmen können dann Gästen Zugang zu dem Web-Portal gewähren: per QR-Code, Beschilderung am Drucker oder Link von Belegschaftsmitgliedern. Gäste müssen dann einfach nur den Link zum Web-Portal auf Ihrem Gerät öffnen, ihre E-Mail-Adresse eingeben und dann das zu druckende Dokument hochladen. Daraufhin öffnet sich eine Druckvorschau, in der sie das Format und weitere Einstellungen (je nach Konfiguration durch den IT-Administrator) anpassen können. Der Zieldrucker wird aus einem Drop-down-Menü ausgewählt. Anschließend kann der Gast entweder sofort drucken oder sich eine E-Mail mit Anweisungen zur Freigabe senden lassen.

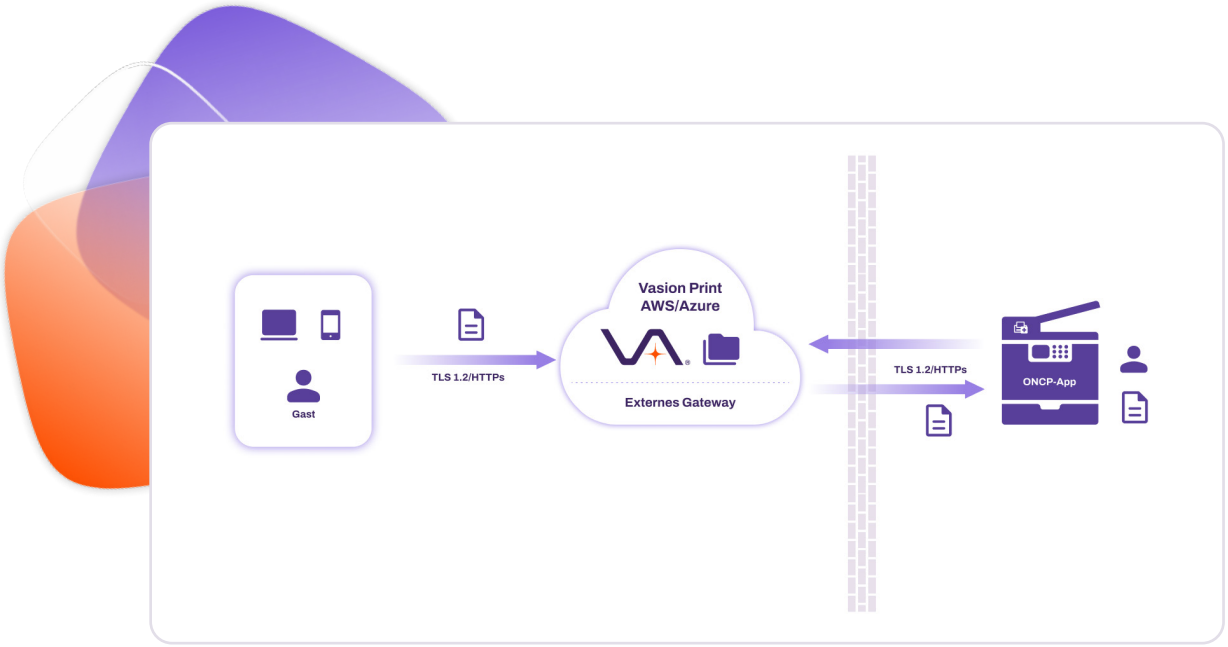

ABBILDUNG 7: Web-Druck-Ablauf für Gastbenutzer mit detailliertem Prozess vom Hochladen des Dokuments über ein BYOD-Gerät (BYOD = „Bring your own device“) in den verschlüsselten Speicher im AWS-Konto von Vasion, gefolgt von der Freigabebestätigung und dem Herunterladen des Dokuments durch die ONCP-App und dem Druck des Dokuments.

Web-Druckaufträge können bis zur sicheren Freigabe zurückgehalten werden, um sensible Dokumente zu schützen, ohne die Netzwerksicherheit zu gefährden. IT-Administratoren können erzwingen, dass alle Druckaufträge von Gastnutzern bis zur sicheren Freigabe zurückgehalten werden, um die sichere Entgegennahme vertraulicher Informationen zu gewährleisten. Für Gäste, die sicheres Drucken nutzen möchten, nutzt die Web-Druck-Funktion die Off-Network-Cloud-Printing-Anwendung von Vasion, d. h., der Druckauftrag wird so lange in der Cloud zurückhalten, bis er vom Gast freigegeben wurde. Dazu können Gäste die Control Panel Application (CPA) verwenden, indem sie einen per E-Mail zugesendeten Freigabecode eingeben. Alle Druckaufträge werden verschlüsselt, sowohl während der Übertragung (per TLS) als auch in der Cloud (AES-256-Verschlüsselung). Dieser sichere Prozess erfordert weder zusätzliche Software noch Zugriff auf Ihr Netzwerk. Gäste benötigen lediglich eine E-Mail-Adresse und den Link zum Web-Portal.

Off-Network Printing

Viele Unternehmen beschäftigen Leiharbeiter, gewähren ihren Partnern Zutritt zu ihren Geschäftsräumen und ermöglichen ihren Mitarbeitern die Arbeit von externen Standorten aus. Diese Personen haben normalerweise keinen Zugriff auf das Firmennetzwerk. Wird ihnen der Netzwerkzugriff dennoch gewährt, birgt dies ein mögliches Sicherheitsrisiko für alle Multifunktionsgeräte im sicheren Netzwerk.

Alle Mitarbeiter, unabhängig von ihrem Standort, benötigen freien Zugriff auf Drucker mit Internetanschluss, die sich hinter der Firmen-Firewall befinden – jedoch ohne die Netzwerksicherheit zu gefährden. Beim Off-Network Printing werden Druckdaten mit TLS 1.2 verschlüsselt. Solange sich zurückgehaltene Druckaufträge, die per Pull-Printing oder sicherem Drucken freigegeben werden können, noch im Netzwerk befinden, bleiben sie verschlüsselt. Off-Network Printing unterstützt Zero-Trust-Anforderungen, um die Sicherheit zu gewährleisten. Das heißt, alle Benutzer müssen ihre Identität vor dem Druck nachweisen.

Diese Lösung leitet Druckaufträge über zwei Komponenten weiter: das externe Gateway und den internen Routing-Dienst.

- **Externes Gateway:** Das externe Gateway empfängt Off-Network-Printing-Aufträge von externen Workstations über HTTPS (Port 443). Die Daten sind dabei per TLS 1.2 verschlüsselt. Das externe Gateway wird von Vasion Print als Service in AWS gehostet. Dabei kann zwischen selbst gehostetem und hybridem Modell gewählt werden. Wenn der Kunde das externe Gateway hostet, wird es auf einem Service-Client ausgeführt und erfordert ein SSL-Zertifikat (Secure Sockets Layer).
- **Interner Routing-Dienst:** Der interne Routing-Dienst läuft auf einem Service-Client innerhalb des Kundennetzwerks und überwacht mithilfe von WebSockets das externe Gateway auf eingehende Druckaufträge über Port 443. Wird ein Druckauftrag an das externe Gateway gesendet, lädt der interne Routing-Dienst ihn sofort über Port 443 herunter und leitet ihn über Port 9100 an den Drucker weiter (oder über Port 631 bei Chromebooks). Wird der Druckauftrag mittels der Funktion sicheres Drucken oder Pull-Printing gesendet, wird er standardmäßig auf der Workstation des Endbenutzers zurückgehalten. Der interne Routing-Dienst kann redundant in

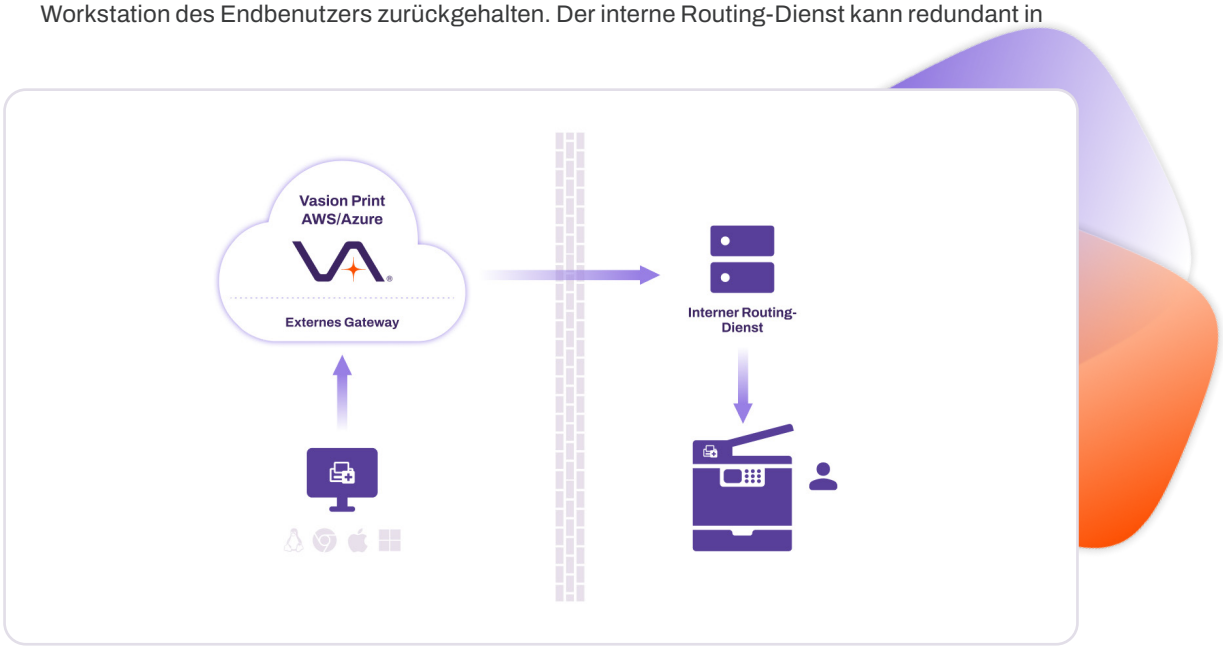

ABBILDUNG 8: Beim Off-Network Printing wird das externe Gateway von Vasion Print in Azure oder AWS gehostet und der interne Routing-Dienst wird lokal durch den Kunden gehostet.

die Umgebung integriert werden.

Off-Network Printing für Mobilgeräte

Mobilgerätenutzer verwenden oft das Funknetz ihres Mobilfunkanbieters. Sie dürfen nicht immer dasselbe Netzwerk nutzen, in dem sich die Drucker befinden. Mit Off-Network Printing können diese Benutzer auf einem sicheren Drucker im sicheren Netzwerk des Unternehmens drucken, indem sie die Druckaufträge über den internen Routing-Service-Client weiterleiten und den Auftrag über direkten IP-Druck an den Drucker senden. Benutzer authentifizieren ihre Identität mittels LDAP oder einem Cloud-IdP und senden Druckaufträge aus der App heraus. Der Auftrag wird mittels TLS 1.2 verschlüsselt und über HTTPS und Port 443 an das externe Gateway gesendet. Das Gateway leitet den Druckauftrag an den Service-Client weiter, indem es den internen Routing-Dienst ausführt. Sobald der Drucker, der für Off-Network Printing konfiguriert ist, bereit ist, den Druckauftrag zu empfangen, leitet der interne Routing-Dienst ihn an den Drucker weiter.

Off-Network Cloud Printing (ONCP)

Der Unterschied zwischen dem Standard-Off-Network-Printing und dem cloudbasierten Remote-Druckansatz ist, wie Druckaufträge weitergeleitet werden. Der Name ist dabei Programm: über die Cloud, sodass kein lokaler interner Routing-Dienst, der auf dem Service-Client läuft, erforderlich ist.

Die Kundendaten werden logisch getrennt in Ordnern des Amazon Elastic File System (EFS) innerhalb der Cloud gespeichert. Druckaufträge werden über einen verschlüsselten Tunnel an das externe ONCP-Gateway von Vasion Print gesendet. Dort erhalten sie ein universell eindeutiges Kennzeichen, um sicherzustellen, dass der Auftrag an den richtigen Ort geleitet wird.

Druckaufträge werden im Cloud-Speicher-Mikroservice in einem verschlüsselten Zustand zurückgehalten, bis sie über das ONCP-Drucker-Gateway gedruckt werden können. Die ONCP-App, die auf dem Drucker installiert ist, ermöglicht den Datenverkehr vom Gateway zum Drucker über WebSocket-Verbindungen (HTTPS oder IPP). Wenn die Druckwarteschlangen bereit für den Auftrag ist, kommuniziert die App mit dem ONCP-Gateway und lädt die Auftragsdaten zum Drucken herunter.

Beim Off-Network Cloud Printing können Druckaufträge für das sichere Drucken oder Pull-Printing zurückgehalten und in einem Cloud-Speicher-Mikroservice zurückgehalten werden, bis die Freigabe erfolgt. Dies ist ein Vorteil, da die Aufträge jederzeit freigegeben werden können und keine Einschränkungen bestehen, wenn die sendende Workstation offline ist. Der Druckauftrag wird nicht kopiert oder zwischengespeichert und aus dem Speicher gelöscht, sobald er freigegeben wurde. So ist die Sicherheit des Dokuments sichergestellt, während sie in der Cloud gespeichert ist.

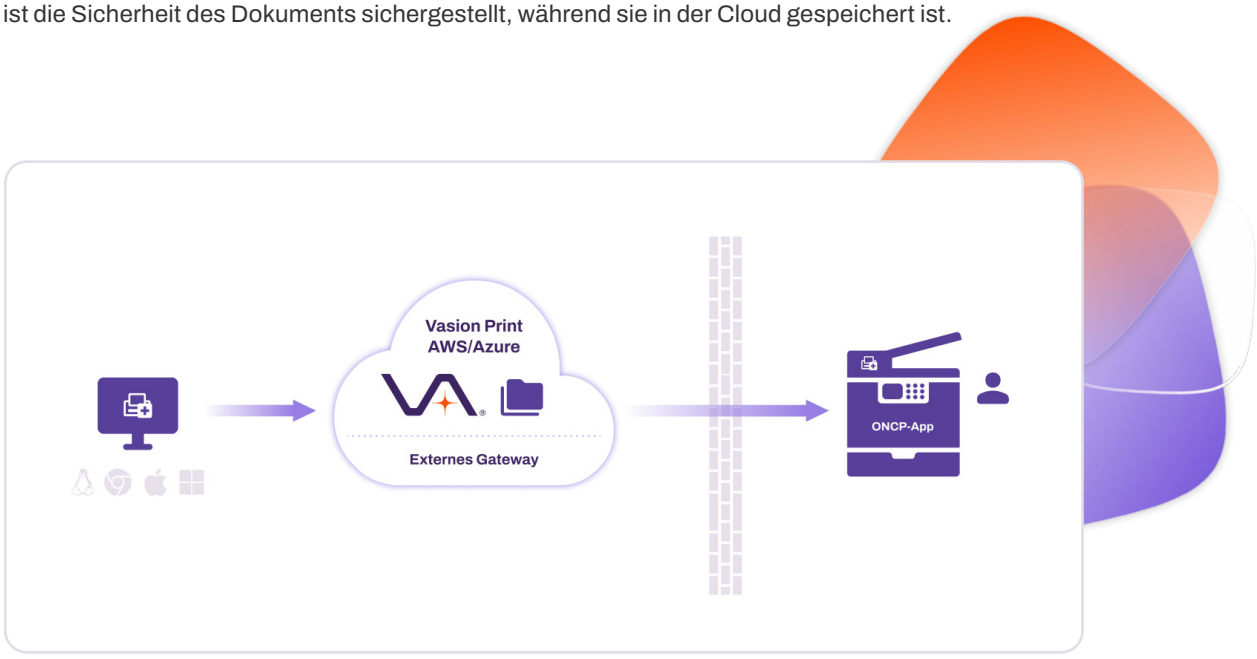

ABBILDUNG 9: Beim Off-Network Cloud Printing von Vasion Print können Benutzer von überall aus drucken, sodass kein lokaler interner Routing-Dienst mehr nötig ist.

Fazit

Jede SaaS-Lösung, die den Fluss und Abruf vertraulicher Informationen steuert, muss sicher sein. Mit Vasion Print wird sämtliche Kommunikation zwischen Workstation-Clients und der in AWS/Azure gehosteten Vasion Print-Instanz per HTTPS und TLS über Port 443 verschlüsselt und mit einem OAuth2-Sicherheitstoken gesichert. Beim Downloads von Treibern erfolgt eine Hash-Überprüfung.

Vasion nutzt die Sicherheitsfunktionen von Amazon Web Services und Azure Cloud, um zu gewährleisten, dass die Vasion-Systeme und -Daten sicher sind und die Vorteile der gemäß ISO 27001 zertifizierten AWS-Plattform nutzen. Darüber hinaus ist die Vasion Print-SaaS-Plattform gemäß ISO 27001:2022 und SOC 2 Type 2 zertifiziert. Dies unterstreicht unsere Verpflichtung, Ihre Daten mit optimierten, effizienten Sicherheitskontrollen zu schützen.

Dank der Direkt-IP-Architektur von Vasion Print bleiben alle Druckaufträge im lokalen Netzwerk, außer beim Off-Network Printing und Off-Network Cloud Printing. Metadaten zum Druckauftrag sind die einzigen Informationen, die über WAN an die gehostete Vasion Print-Instanz gesendet werden. Vasion Print ist mit einem oder mehreren IdP-Services integrierbar, um Benutzer, Gruppen und Computer zu authentifizieren und zu autorisieren. Sofern vom IdP bereitgestellt, ist auch eine Mehrfaktor-Authentifizierung möglich. Vertrauliche Daten werden zudem durch eine Reihe von sicheren Pull-Printing-Funktionen geschützt.

Vasion Print bietet eine hoch verfügbare, serverlose Druckplattform, dank der IT-Administratoren Druckserver komplett abschaffen können. Die SaaS-Lösung strukturiert die vorhandene Druckumgebung so um, dass zentral verwalteter, direkter IP-Druck möglich ist. Sie bietet Druckerbereitstellung und -management, Druckprüfung und -berichte sowie zentrales Druckmanagement – alles über eine webbasierte Konsole. Und wie sieht es mit der Kosteneffizienz aus? Die Erfolgsbilanz hinsichtlich des Return-on-Investment von Vasion überzeugt: Kunden berichten von messbaren Gewinnen durch Reduzierung der Infrastruktur, bessere IT-Effizienz, optimierte Verfügbarkeit/Zuverlässigkeit von Druckern und geringere Helpdesk-Kosten.

VASION®

11894|Feb 2025

Glossar Abkürzungen

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: Gruppenrichtlinienobjekt

HTTPS: Hypertext Transfer Protocol Secure

IdP: Identitätsanbieter

IMAP: Internet Message Access Protocol

IPP: Internet Printing Protocol

JIT: Just In Time

LDAP: Lightweight Directory Access Protocol

LDAPS: Lightweight Directory Access Protocol (über SSL)

MFA: Mehrfaktor-Authentifizierung

NAT: Network Address Translation

OAuth2: Open Authorization 2.0

OIDC: OpenID Connect

ONCP: Off-Network Cloud Printing

ONP: Off-Network Printing

PII: Personenbezogene Daten

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