White Paper

# Zscaler For Users Healthcare Deployment Strategy

# Contents

## Summary

This document is intended to discuss the use cases most commonly seen in healthcare and the deployment strategy with Zscaler for those use cases.

## Intended audience

| Typical Audiences | |
|---|---|
| **Roles** | **Responsibilities** |
| Security Manager | Leader who oversees security measures within an organization. Security managers with a focus on cybersecurity manage IT teams and develop strategies for cybersecurity efforts. They may also write rules and regulations regarding cybersecurity decisions. |
| Network Security Engineer | Helps implement security measures that apply to connections to the network and how a computer protects its information over the internet. |
| Security Engineer | Implements important security measures across an organization. The security engineer may troubleshoot new security measures. They often coordinate the response to breaches in security and help the IT team develop solutions for avoiding those breaches in the future. |
| IT Administrator | General IT Administrator or user responsible for a specific domain included in a Zscaler deployment. |
| Application Director | Responsible for the delivery of applications throughout the healthcare facility. These include end user productivity applications, EPR systems, and Electronic Medical Record systems which include all aspects of patient care. |
| Application Analyst | Responsible for the configuration and integration of applications across the continuum of care. Examples of these include EMR, PACs, cardiology, and speech recognition applications. |

## Use cases

In healthcare, use cases can be grouped into two separate descriptions:

- Clinical use cases – Clinical is defined as anything that can impact a patient while they are being cared for. Any service outage or degradation assumes the highest priority to restore any services that impact direct patient care.
- Non-clinical use cases – Non-clinical is defined as roles that are not directly impacting patient care.

In most cases, electronic medical record (EMR) software that is deployed has a heavy influence on the other supporting applications for the EMR platform. Organizations must create an application delivery strategy by understanding user requirements and how applications are consumed at the point of care while also maintaining compliance and security standards.

Most healthcare providers deliver EMR platform software in the form of published applications via traditional VDI environments. They may publish these from an on-prem data center or through a direct connection to a cloud-hosted provider. In some cases, these published applications will be deployed so they are internet-facing. Zscaler's zero trust approach eliminates the need for external facing applications such as EMRs by utilizing Zscaler Private Access (ZPA). We connect the user to the application, not the network.

We also offer posture control, context, inline DLP, Secure Web Gateway, NGAV, firewalling, SSL decryption, and other security products all wrapped under a single umbrella. This means users can access their applications not just from anywhere but securely to avoid breaches and data leakage. This eliminates the need for point solutions by offering consolidation and end-to-end visibility.

## Common use cases for Zscaler in healthcare environments

| Common Use Cases | |
|---|---|
| **Use case** | **Description** |
| Nurse Kiosk | Central location for care team members to meet and discuss rounding and patient care needs. EMR access is typically through a shared workstation with a tap-and-go login |
| Patient Room | Patient room typically uses a device such as an iPad to access applications or care notes in an effort to deliver a personalized patient experience. |
| Medical Imaging | Use for diagnostics of radiology or other medical images. Typically require specialty hardware for image review. Subject to review and certification by the FDA to ensure lossless images. |
| Clinical Research | Research related to AI/ML, genomics, population health, and others. Though the EMR is leveraged by researchers, the most time is spent extracting and working with the data from the EMR and integrating them into an enterprise data warehouse. Can be contracted doctors and not employees. |
| Non-Clinical Staff | Diverse application needs—includes groups such as IT, HR, finance, etc. |
| Non-Clinical Kiosk | Used in reception and front desk areas. Patients can self-register, pay bills, and do other controlled activities related to their medical visit. |
| Remote Workforce | Anyone outside of direct network connectivity such as rural doctor offices, mobile doctors, work from home, etc. |
| M&A | Hospitals that are buying other hospitals and need to integrate them into existing environments. |
| Epic Community Connect | Larger hospital networks can license Epic's software to smaller hospitals for less cost than a standard Epic deployment. This is usually a use case for smaller than 200-bed hospitals. |

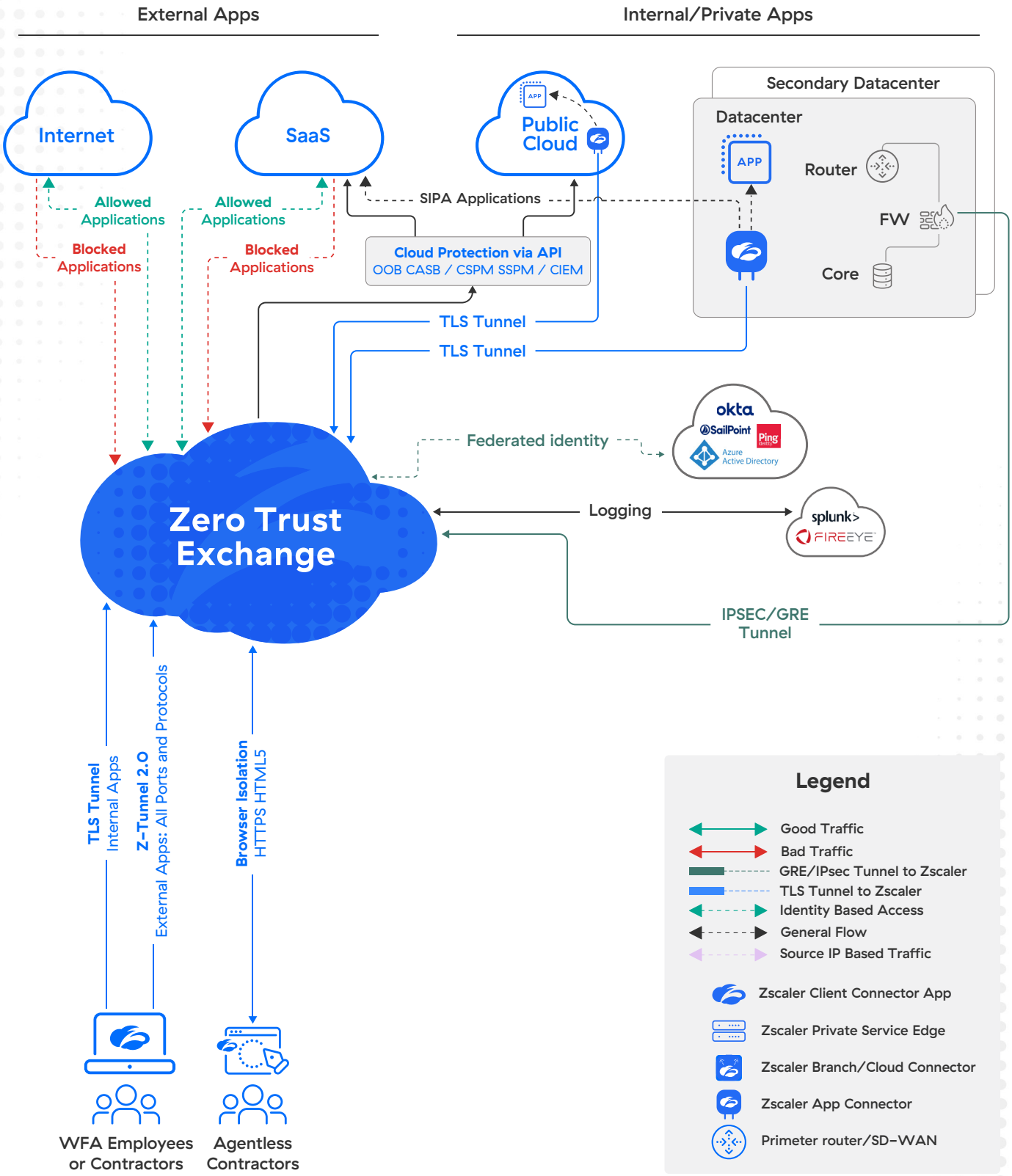
## Remote workforce / VPN replacement

Zscaler leverages a cloud-native architecture, meaning it operates entirely in the cloud without the need for on-premises infrastructure. This eliminates the complexity and maintenance associated with VPN hardware and software, reducing costs and providing scalability. Zscaler also provides access to your cloud-based applications without the need to route through your internal data center. While some applications such as a cloud-hosted EMR platform may have a direct connection in an effort to lock down access to only on-prem connections, Zscaler can connect directly to that cloud provider and provide native access.

VPN hardware can create a bottleneck of performance issues or single points of failure, Zscaler's global cloud infrastructure ensures scalability and high performance. It can handle increased user demand and traffic without affecting the user experience. Additionally, the distributed architecture reduces the dependency on a single point of failure, providing high availability.

Unlike VPNs that provide network-level access, Zscaler's ZTNA enables granular access control to specific applications or resources, reducing the attack surface. Zscaler's ZTNA solution enforces strict security policies based on user identity, device health, and other contextual information. It verifies each connection request, ensuring that only authorized users and devices can access specific applications or resources. Additionally, Zscaler's cloud-based platform performs real-time threat analysis and applies advanced security controls to protect against malware, zero-day exploits, and data exfiltration.

## Logical design of work from anywhere using Zscaler



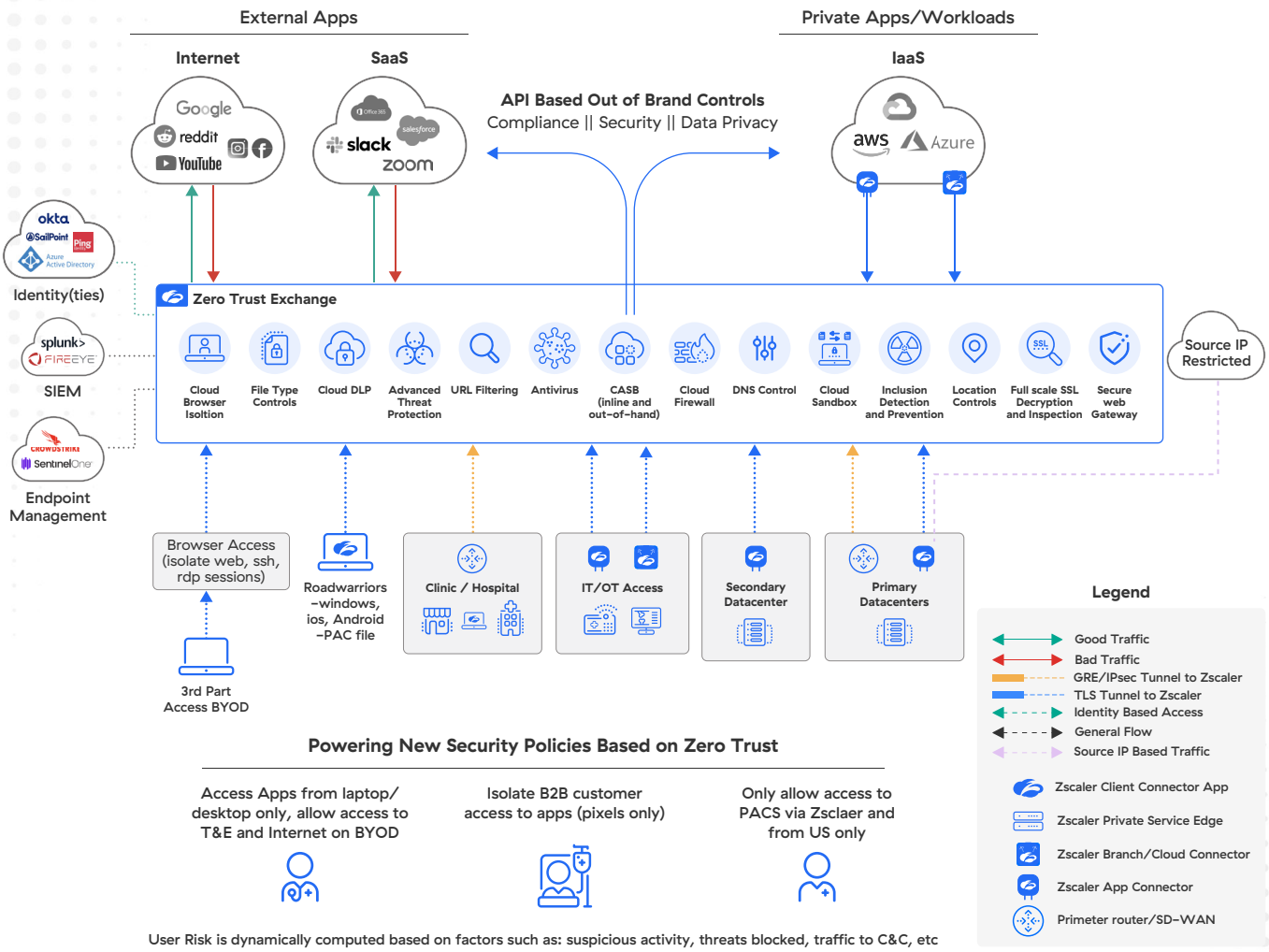
## Access clinical apps without MPLS

Zscaler provides a solution called Zscaler Private Access (ZPA) that enables secure access to clinical applications like Electronic Medical Records (EMR) without the need for an MPLS circuit. To access clinical applications, you need to deploy a ZPA Connector within your network, which can be deployed via a lightweight VM or a physical RHEL machine. The connector acts as a secure bridge between your local network and the Zscaler cloud. It establishes an outbound connection from your network to the ZPA service.

You can then define specific access policies based on user identity, device posture, and other contextual factors. ZPA integrates with your existing identity provider (IdP) or uses its built-in authentication mechanism to verify user identities before granting access. This ensures that only authorized users can access the clinical applications. This also allows provisioning to be fast and simple. Zscaler Client Connector can auto-enroll with ZPA and auto-login, taking out steps between the clinician and the client.

When a user requests access to a clinical application, the ZPA Connector establishes an encrypted connection to the Zscaler cloud. The cloud acts as a proxy and forwards the request to the targeted application. This way, the application is not exposed to the public internet. Your user's session will only be connected to the applications they have access to and will not be allowed to move laterally throughout the network.

Logical design of site to site connectivity using Zscaler



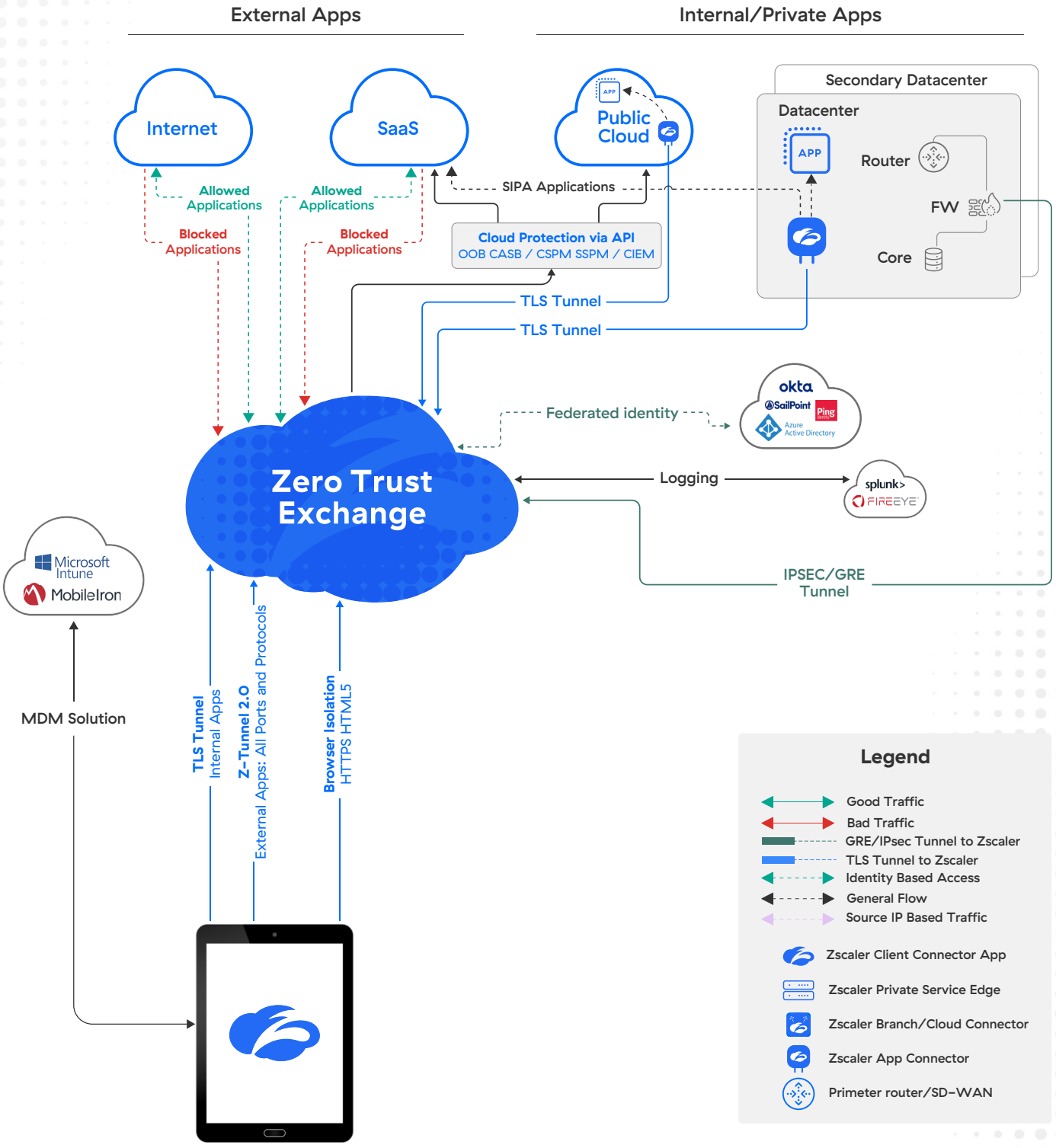

## Patient or clinical mobile devices

Zscaler also offers Client Connector for IOS and Android devices. The app acts as a secure gateway, redirecting all internet traffic from the device through the Zscaler cloud. This ensures that all data transmitted to and from the mobile device is inspected and protected. Zscaler's cloud-based Secure Web Gateway (SWG) provides web filtering and threat protection capabilities. It enforces security policies, blocks malicious websites, and scans web content for malware or other threats.

Zscaler's DLP features help prevent data leakage from mobile devices. It monitors outgoing traffic and applies policies to detect and prevent the unauthorized transmission of sensitive data, such as personal health information (PHI) and confidential documents. This ensures compliance with data protection regulations. Zscaler also leverages advanced threat intelligence and real-time analysis to detect and block malware, phishing attacks, and other threats on mobile devices. The traffic passing through the Zscaler cloud is inspected for known malicious patterns, suspicious behavior, and zero-day threats, providing an additional layer of security.

Zscaler integrates with Mobile Device Management (MDM) solutions to enforce security policies and manage mobile devices more effectively. This integration allows IT administrators to apply device-level controls, such as password requirements, device encryption, or remote wipe capabilities, ensuring devices meet security standards.

### Logical design of mobile devices using Zscaler



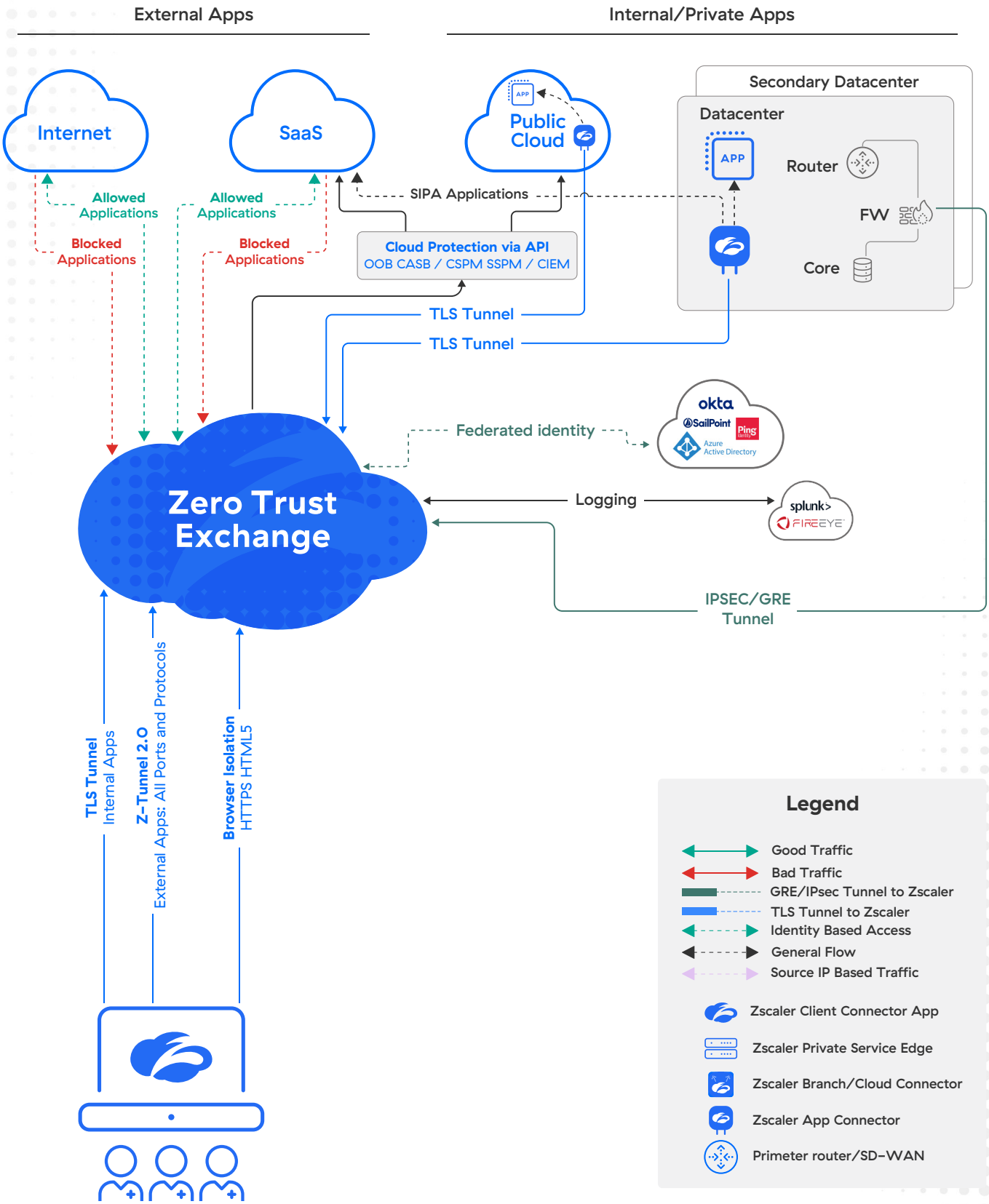
## Patient and clinical kiosk/shared workstation

Zscaler can secure kiosk/shared workstations by installing Zscaler Client Connector on them. Often, these will be machines either in the waiting room or in a patient's room that a nurse will log into. These kiosks typically have a limited set of applications that they have installed but require protection from outside threats. Email, web browsing, and using an EMR can be done on most kiosks in a patient's room or at a nurses' station on the floor. By utilizing Zscaler Client Connector, paired with ZPA and ZIA, we can ensure a safe and secure connection between the workstation and any internet destination such as public cloud, private cloud, or web browsing.

Zscaler offers session management capabilities that help control and monitor user sessions on shared workstations or kiosks. Administrators can set session timeouts, enforce session termination upon inactivity, and track user activity to prevent unauthorized access or misuse. Zscaler's Secure Web Gateway (SWG) inspects web traffic from shared workstations or kiosks. It applies web filtering policies to block access to malicious or inappropriate websites, SWG also scans web content for malware, protecting shared workstations from downloading infected files.  Zscaler's Cloud Firewall enforces firewall rules and blocks unauthorized connections. The Cloud Firewall adds an additional layer of security to the shared environment.

Zscaler's DLP features can help prevent data leakage from shared workstations or kiosks. It monitors outgoing traffic and applies policies to detect and prevent the unauthorized transmission of sensitive data, such as patient information or confidential documents. DLP also ensures compliance with data protection regulations.

## Logical design of kiosk machines using Zscaler



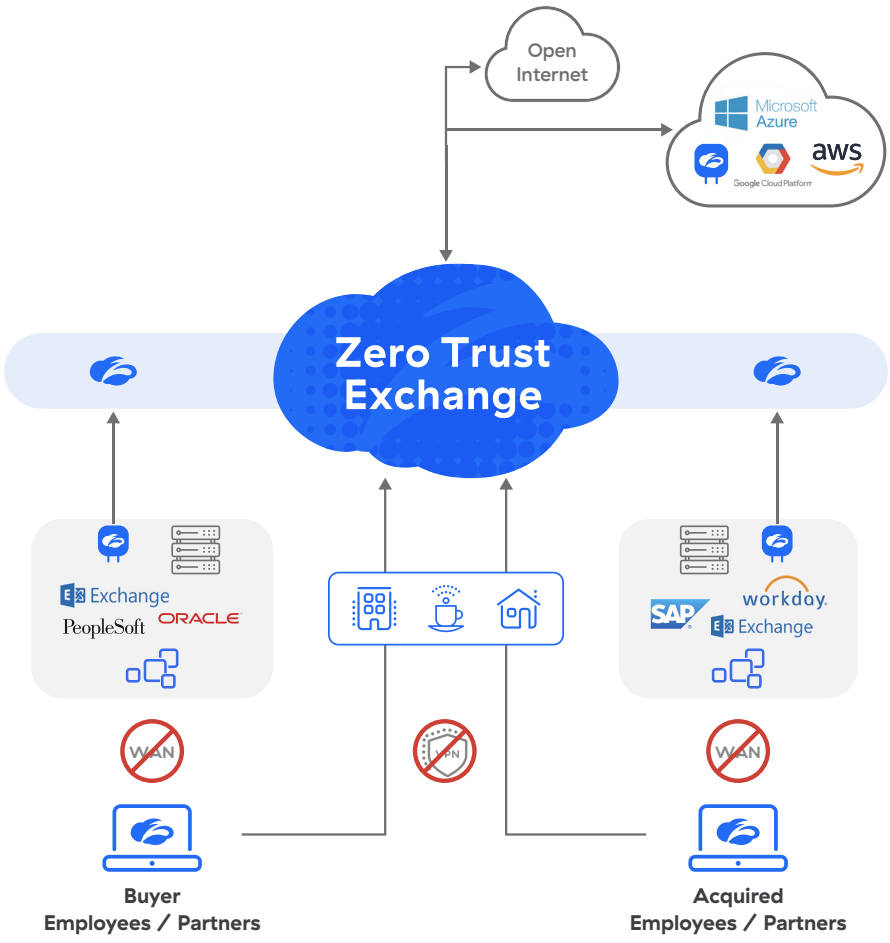
## Mergers and acquisitions

The traditional approach of mergers and acquisitions often requires things such as new security assessments, integrating target and parent networks, application access predicated on network access, and domain joining. This can lead to increased lateral movement threats from parent to target hospitals, longer lead times due to needing to integrate the network first, and collaboration or application access being delayed.

Zscaler ZTNA allows for accelerated time to value by providing network access via a zero trust architecture to your parent network from the target network. With ZTNA, you are able to mitigate and control risks by using posture controls within the administrator console. Zscaler allows the ability to simplify the solution by reducing the many integration points of security tools such as firewall rule sets, VPN access, device settings, etc.

We achieve this by first deploying a Zscaler tenant, Client Connector, and App Connector to sit in line with user traffic. We can then use real traffic data to identify the usage level of key applications. This leads to implementing and enabling access policies around these retained applications. You then are able to optimize staffing and consolidate point solutions. Finally, you would be able to expand or collapse your Zscaler integration tenant.

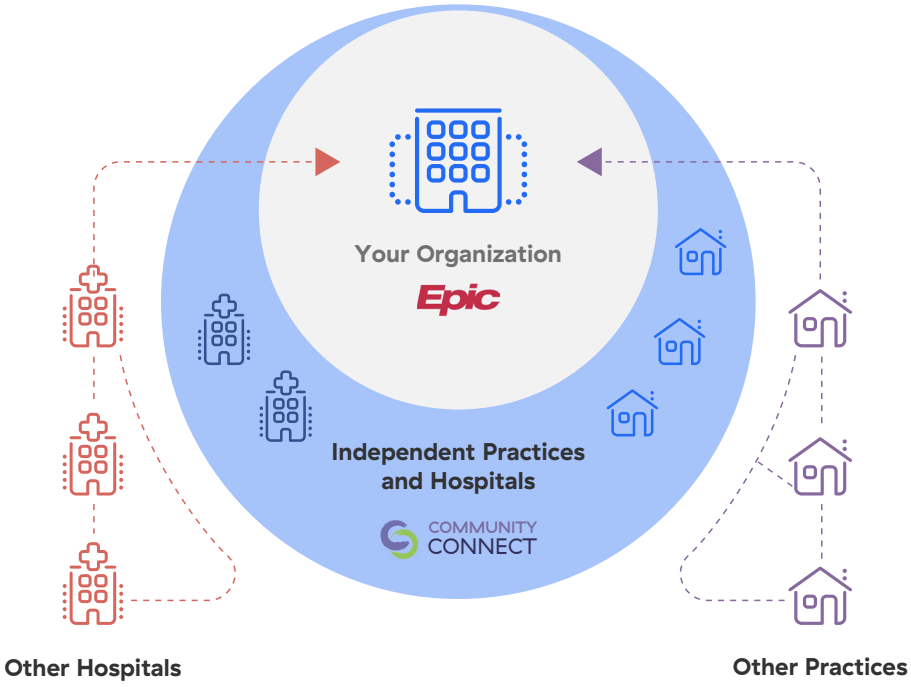
**Logical design of mergers and acquisitions using Zscaler**



## Epic Community Connect

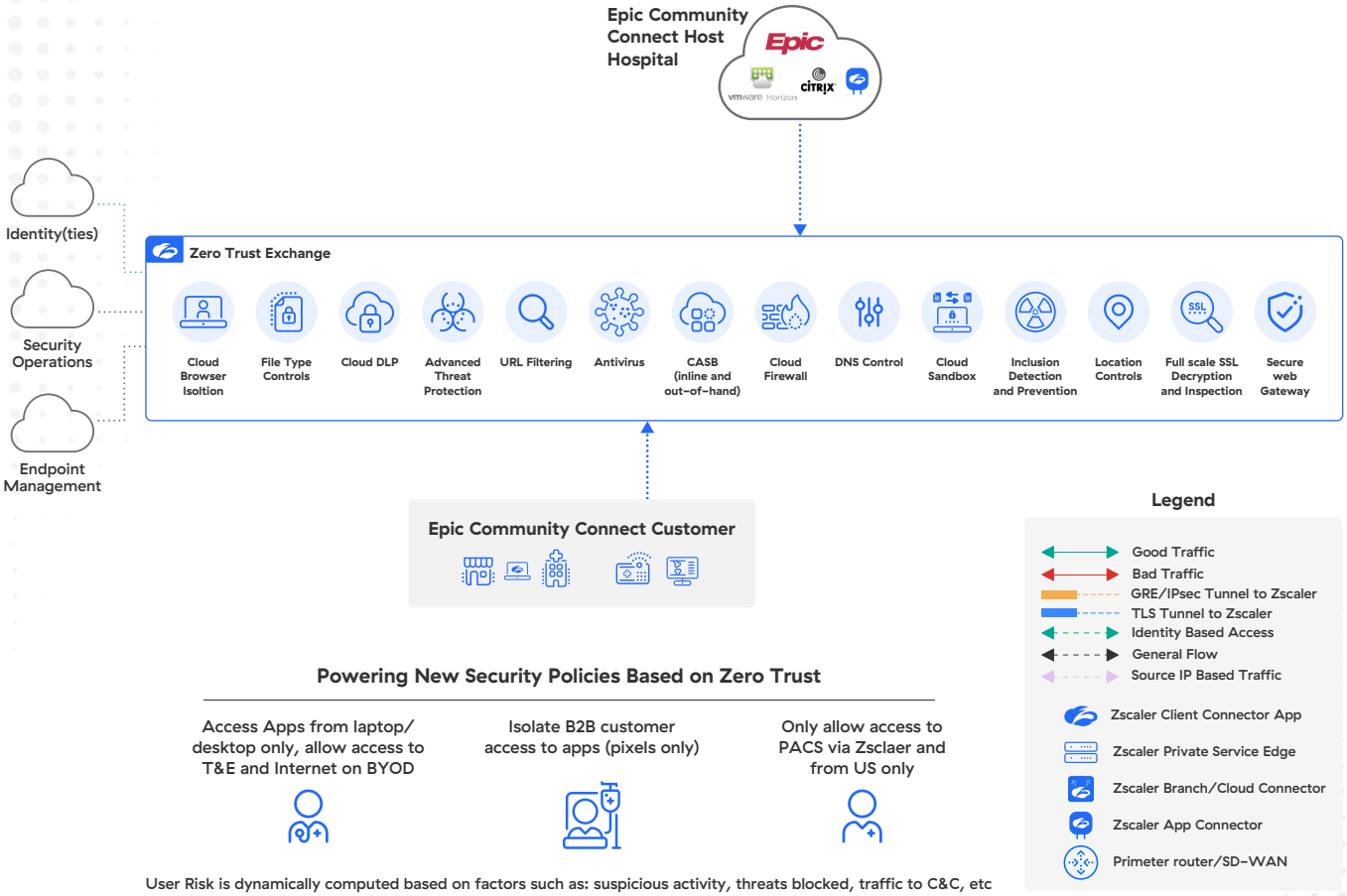
Epic Community Connect is a program through Epic in which they give the ability to allow larger hospital networks to license out Epic's platform to other smaller hospitals. The goal is to decrease the cost of an Epic implementation for a smaller hospital network while also giving the host hospital the ability to do a chargeback model. In this particular case, the host hospital would be responsible for all of the SLAs and support for the buying hospital.

### Epic Community sample diagram



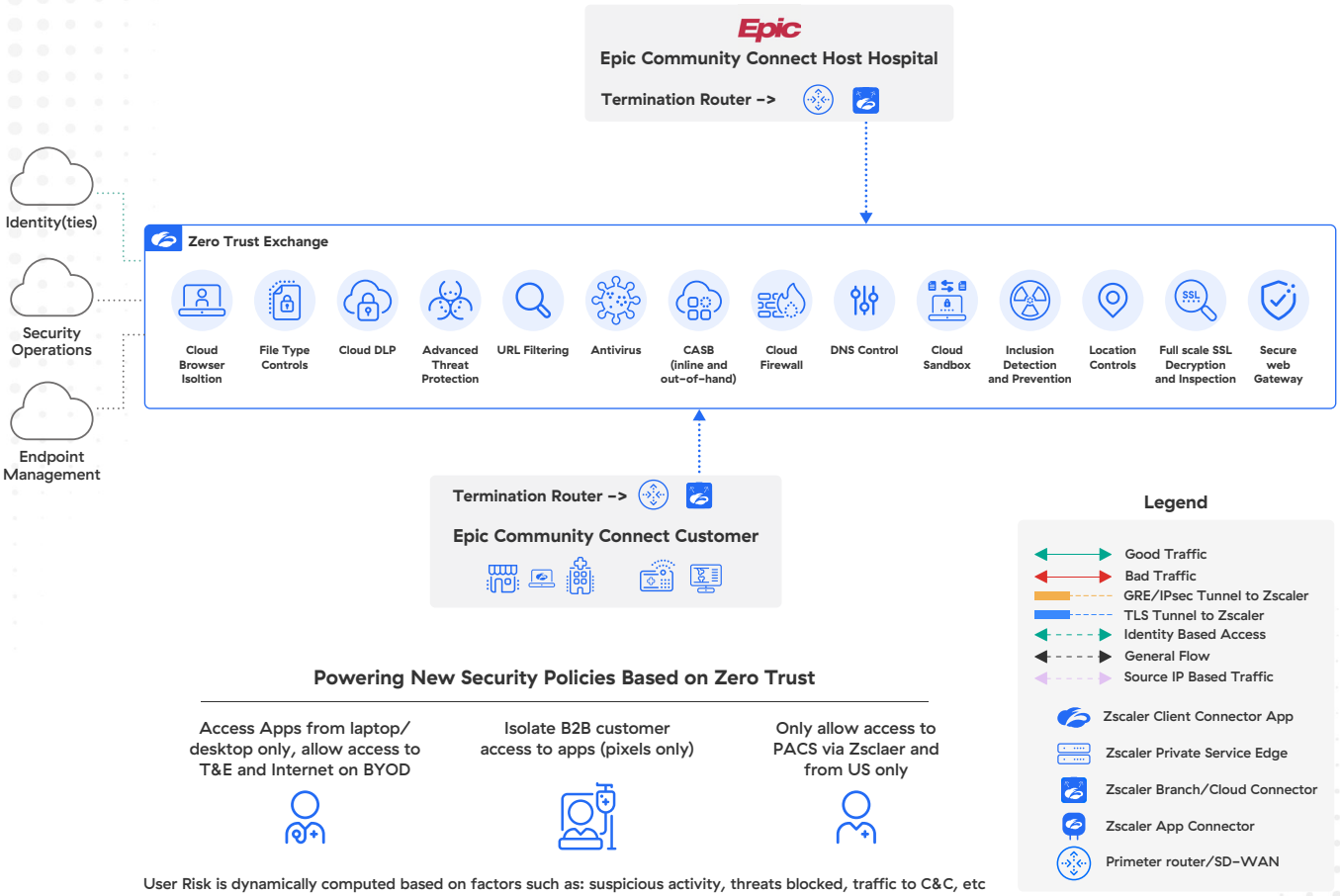

Zscaler offers two solutions to ensure these hospitals get onto the host hospital's infrastructure safely. The first is a standard Zscaler Private Access use case. The host hospital would deploy an app connector within their data center while giving out Zscaler Client Connector to the buying hospital. This will allow the hospital to get onto the network and launch Epic without ever needing an external facing gateway. You will still need to deploy Epic to their best practices usually done through a published application but this will eliminate the need for a VPN or an external-facing portal. As most customers print within Epic, you will need to set up either Local Virtualized Printing in which Epic sends a PDF document to the local machine to print via a local printer or, a local printer set up within Epic. Both are supported methods of printing within Epic.

## Logical design of Epic Community Connect using Zscaler




If your company has the need to use IoT devices that cannot have the Zscaler Client Connector installed on them, then the second option you have for deployment would be to utilize Zscaler Branch Connector. This solution requires a small lightweight appliance to be installed in a virtualized environment either KVM or VMware ESXI. This will create a tunnel from your host hospital to the buyer hospital. You will require a router at both ends as well to receive this traffic, however, it does not need to be an MPLS circuit. Some customers can choose to buy a CPE device that contains the necessary switching and ability to install a lightweight hypervisor all in one device. A sample manufacturer would be Lanner. Please note that Zscaler does not support the hardware or the underlying hypervisor in these deployments and it would be up to the customer to ensure patching is done on both hardware and hypervisor. This gives you the ability to route traffic to Zscaler and then to the Branch Connector appliance on the other side.

Logical design of Epic Community Connect using Zscaler Branch Connector




## Points of integration

**Identify:**

Zscaler uses identity providers such as Okta, Ping, Azure Active Directory, ADFS, and others to provision and authenticate users. Zscaler supports up to 16 different SAML IdPs per organization. You have two methods to provision users within the Zscaler console for provisioning users SAML Auto-Provisioning and System for Cross-domain Identity Management (SCIM).

SAML Auto-Provisioning allows you to provision users based on an authentication event. When a user changes group or adds groups, the database will be updated upon authentication request by that user. SAML Auto-Provisioning is supported by most IdPs out of the box and requires limited configuration. The disadvantage is that users will not be deleted automatically when using SAML Auto-Provisioning.

System for Cross-domain Identity Management (SCIM) offers the ability to auto provision users without the need for an authentication event. SCIM APIs will talk back to the IdP and the Zscaler Admin portal to update users' information, including deprovisioning users. The disadvantage of SCIM is it is not supported by all IdPs.

**Security Information Event Management (SIEM):**

Zscaler seamlessly integrates with leading Security Information and Event Management (SIEM) solutions to enhance your security operations workflows. You can integrate Zscaler with supported SIEM solutions to transmit logs in real time. SIEM integration provides visibility in a centralized console and allows your teams to leverage the solution's existing security investigation workflows.

**Endpoint Security:**

Zscaler integrates with industry-leading endpoint solution partners to provide zero trust access control based on device posture as well as enhance detection, investigation, and response capabilities—no matter where users and apps are—through telemetry and intelligence sharing. We do this by deploying Zscaler Client Connector alongside your cloud native EDR/EPP sensors. The endpoint sensor sends events to the cloud for adaptive machine learning based on posture. When an indicator of compromise data feeds into the Zscaler Zero Trust Exchange, that event will help protect all users.

**Mobile Device Management (MDM):**

Companies use an MDM solution often to control a device whether corporate or BYOD. These devices enroll into the MDM solution and get applications installed. Zscaler Client Connector can be deployed fast and at scale through your chosen MDM solution. We support a wide variety of attributes such as "cloudname", "domainname", and "username" to make this deployment more seamless requiring limited interaction from the end user. Companies may take this approach vs the traditional approach of having IT install the software manually.

## Sample Integration:

### Imprivata

Imprivata is a market leader with their OneSign tap-and-go solution. This solution allows an IT department to provision "kiosk machines" (type 2 Imprivata install) with generic service accounts logged in to Windows. The nurse or doctor would walk up to the machine with their badge and tap it on the card reader. This would then allow them to seamlessly run apps under their user context without ever logging into the machine in a traditional Windows OS fashion. Primary use cases in a clinical setting would be Emergency Rooms, Operating Rooms, and many more patient care settings where quick access to an application for a roaming clinician is required. At the same time, Imprivata improves operational efficiency of the IT staff because workstations can be placed back into service compared to a non-Imprivata workstation in the same deployment.

Our current options with Imprivata

**Option 1:** PAC file and IWA (Integrated Windows Authentication) or a PAC file and second login prompt for Zscaler

**Option 2:** GRE Tunnel from source subnets with a defined location

**Option 3:** Leveraging the service account signed into Windows for identity (S-LOCATION-TAG), ASSET to APPLICATION policy can be created in Zscaler
As an example – providing service account S-LOCATION-TAG access to:

- All Microsoft O365 services
- Company approved payroll sites
- ServiceNow for ticketing
- Facebook Workplace – allow but not post (unless in Marketing)
- Block level 5 and above cloud applications
- Caution level 4 cloud applications

### CrowdStrike

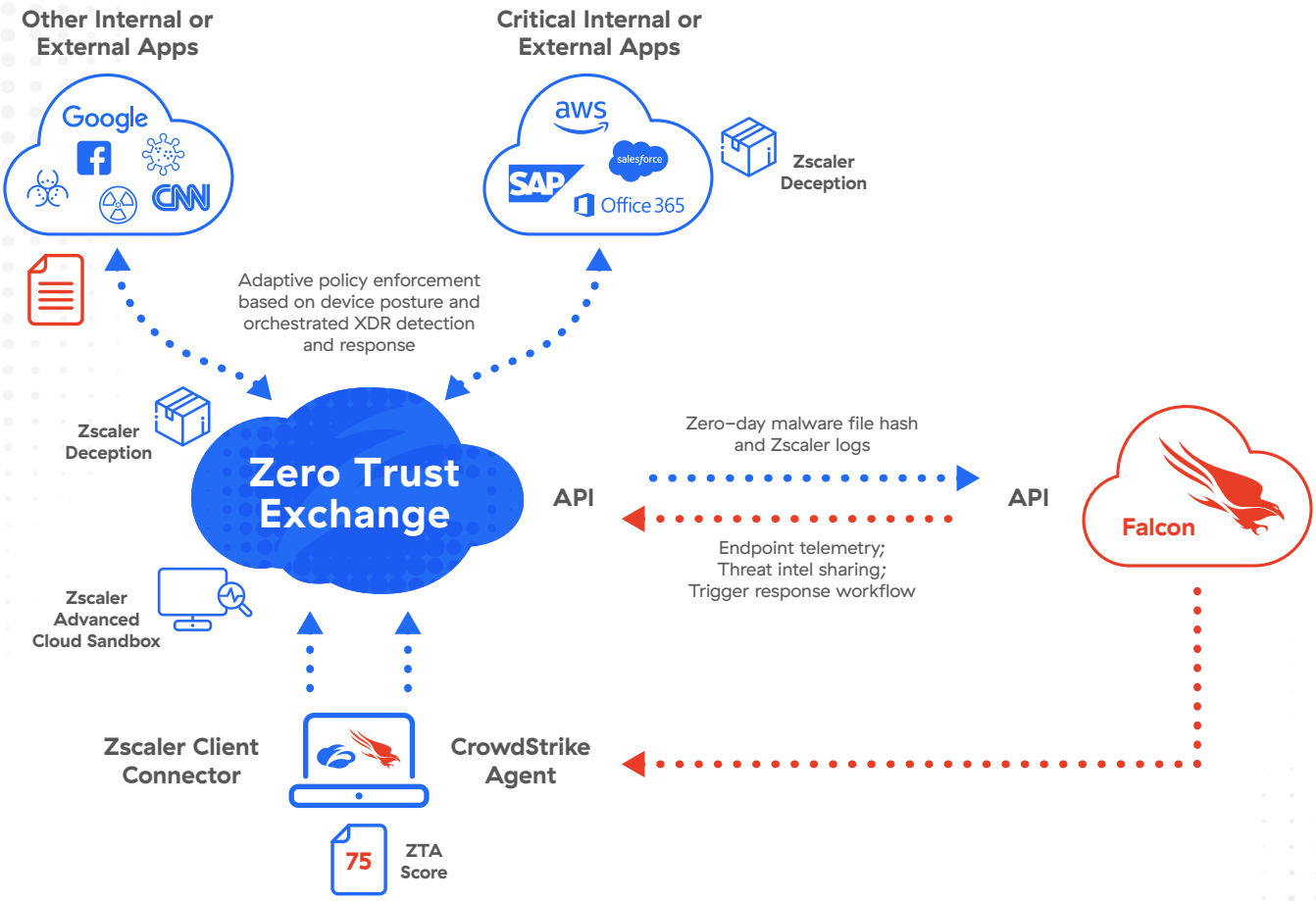
Crowdstrike is an MQ leader in Endpoint Protection, which when utilizing their product and our products, we can share threat intel, device posture, telemetry, and XDR-enabled threat detection.

Utilizing CrowdStrike's Zero Trust Assessment (ZTA) we can block access for non-compliance and rogue devices. CrowdStrike can gather new threat intelligence (IPs, Domains, and URLs) and share with Zscaler to create new block lists.

Zscaler advanced cloud sandbox intercepts inline and detects zero-day malware which then will share file hash with CrowdStrike Falcon to retrieve a list of impacted endpoints in the environment. Zscaler triggers a response by requesting Falcon to quarantine the endpoint or by pivoting to Falcon console for further investigation.

Zscaler shares telemetry with CrowdStrike to enable enhanced visibility and detection capabilities. CrowdStrike initiates cross-platform response workflows by adding in the user gathered from telemetry data to the restrictive group. Zscaler then can restrict that user access to selected critical applications preconfigured for that group.

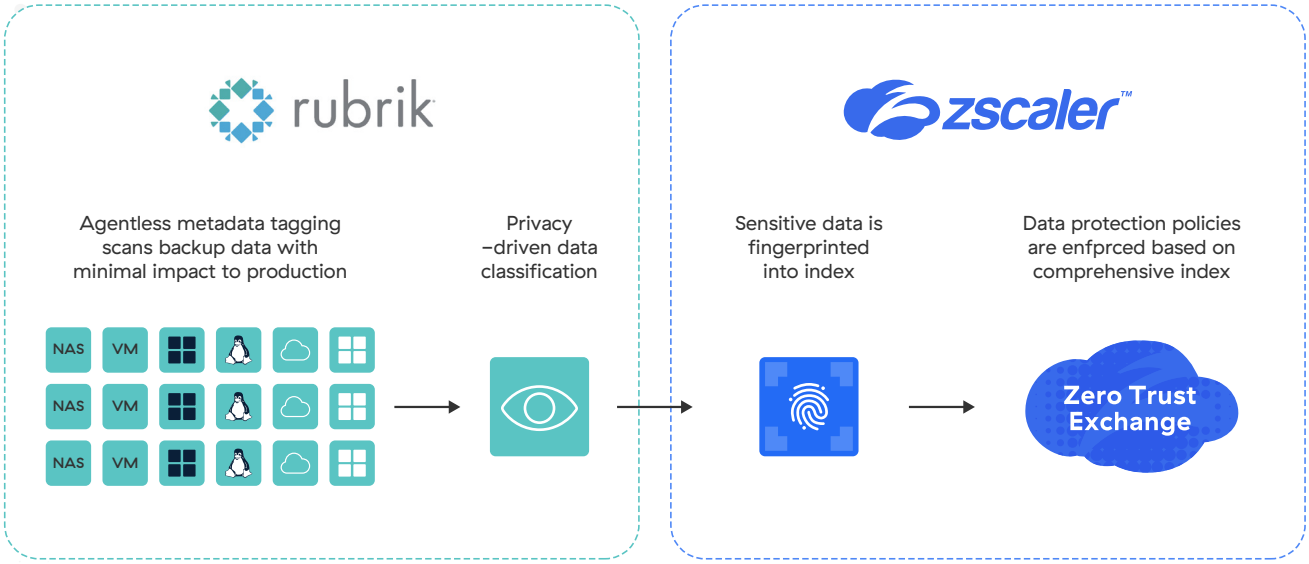
CrowdStrike and Zscaler integration diagram




## Rubrik

With more distributed users and data, organizations are struggling to ensure that sensitive data is not accidentally exposed or deliberately exfiltrated for double extortion attacks. One of the leading sources of data risk in organizations is the inadvertent transmission of sensitive data over the network. Furthermore, malicious encryption of data can be a challenge without a way to keep data safe and make it fast and easy to recover. Rubrik's integration with Zscaler proactively identifies sensitive business data across enterprise, cloud, and SaaS environments so that it can be fingerprinted into an index to more easily and accurately prevent data loss.

## Rubrik and Zscaler integration diagram




Rubrik's unique backup architecture also keeps data safe, accelerates response by understanding data threats, and restores impact data faster, safer, and with confidence. Together, Rubrik and Zscaler place valuable data security insights in the hands of even more security and compliance teams to strengthen data protection policies and prevent the loss of critical business data.

For more information please visit our healthcare page at **zscaler.com/industries/healthcare**

zscaler™ | Experience your world, secured.™

**About Zscaler**

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.



+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com