

# Cloudi-Fi integration within Zscaler ZIA

Empower your Zscaler with a compliant identity provider for guest, BYOD and IoT

## KEY FEATURES OF OUR SOLUTION

- Extend existing Zscaler tenant to guests, BYOD and IoT with total control and visibility
- Suitable to authenticate corporate guests, BYOD and IoT but also customers with hotspots
- Personalized users onboarding and security
- Compliance with local regulations (Data privacy and Internet provider regulations)
- Captive portal service for Hotspots and Retailers
- Quick & frictionless deployment using existing infrastructure

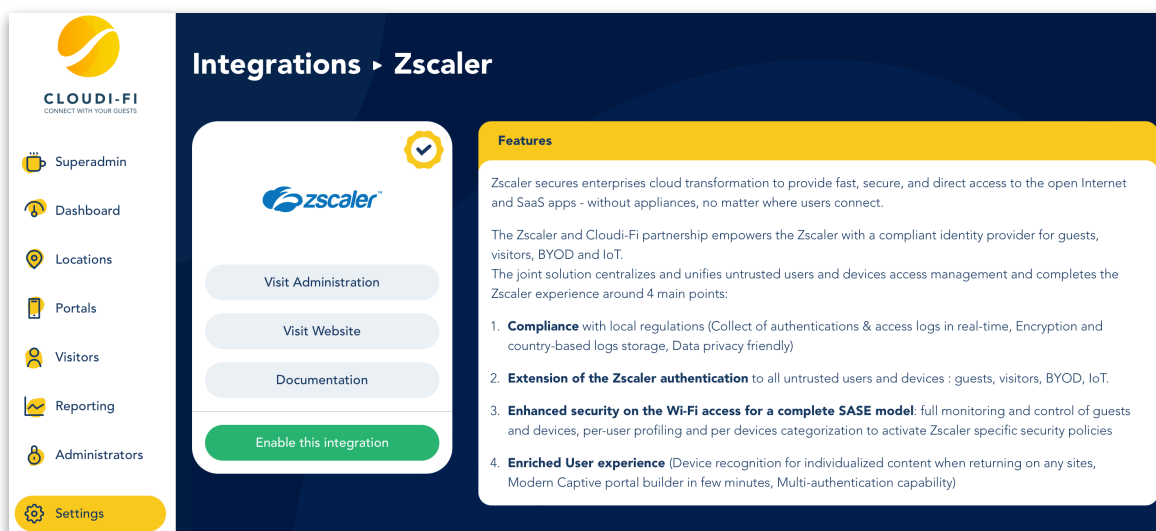
## INTEGRATIONS

- Cloudi-Fi
- Zscaler ZIA

The rise of cloud adoption by enterprises has **democratized distributed networks** in Enterprise. As Internet is eating corporate networks, local Internet breakouts with SD-WAN and Wi-Fi are becoming essential (and often sufficient) to users' connectivity and productivity.

Distributed networks by nature are promoting **cloud based services** gradually replacing central infrastructure. Zscaler **authenticates and secures employees and their managed devices**. Still the lack of complete and accurate identification of users (such as consultants, freelancers, and employees with BYOD) but also untrusted devices like IoT makes them continue to authenticate on central infrastructure (controller, anchor controller, NAC...). And in the same time consuming bandwidth resources unnecessarily and adding complexity in managing those users and devices.

Cloudi-Fi is **extending the authentication capability** of Zscaler to authenticate (and secure accordingly) all users and devices, including BYOD and IoT. This is particularly relevant to existing Zscaler ZIA customers who are one click away of this capability.



**Integrations > Zscaler**

**Features**

Zscaler secures enterprises cloud transformation to provide fast, secure, and direct access to the open Internet and SaaS apps - without appliances, no matter where users connect.

The Zscaler and Cloudi-Fi partnership empowers the Zscaler with a compliant identity provider for guests, visitors, BYOD and IoT.

The joint solution centralizes and unifies untrusted users and devices access management and completes the Zscaler experience around 4 main points:

1. **Compliance** with local regulations (Collect of authentications & access logs in real-time, Encryption and country-based logs storage, Data privacy friendly)
2. **Extension of the Zscaler authentication** to all untrusted users and devices : guests, visitors, BYOD, IoT.
3. **Enhanced security on the Wi-Fi access for a complete SASE model**: full monitoring and control of guests and devices, per-user profiling and per devices categorization to activate Zscaler specific security policies
4. **Enriched User experience** (Device recognition for individualized content when returning on any sites, Modern Captive portal builder in few minutes, Multi-authentication capability)

Zscaler integration into the Cloudi-Fi administration interface

# HOW IT WORKS

Cloudi-Fi is a 100% cloud-based SaaS solution that **centralizes and unifies Guests, BYOD and IoT access management**. It seamlessly integrates within Zscaler and is particularly suited for **SD-WAN** architectures with local internet breakouts.

Cloudi-Fi increases **visibility, compliance and control** of Internet usage by all users.

## Identify your users for a personalized experience

Easily **identify** and **personalize** your guests and visitors.  
**Profile your users** to apply specific **security policies** and adapt your Wi-Fi usage accordingly.

## Multiple authentication modes can be combined:

employee sponsorship, SMS, QR code, social networks, Teams, Slack ... . User will be **automatically recognized** for future visits.

## IoT

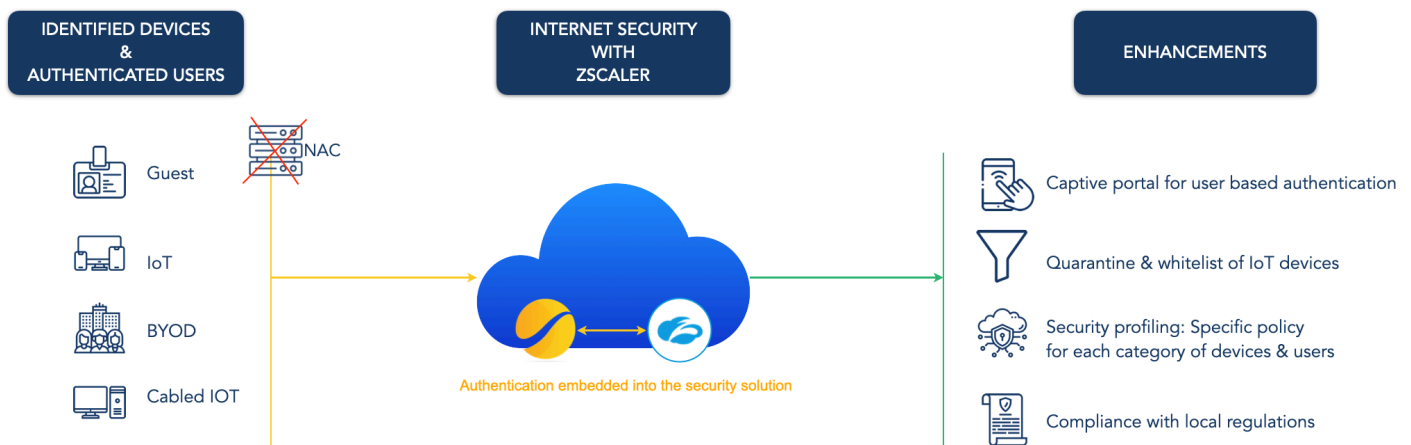
Cloudi-Fi manages IoT access, security and compliance. With its cloud-based DHCP service, Cloudi-Fi provides **discovery, identification and classification** of all IoT devices. In combination with Zscaler, the solution allows IoT-specific security policies in line with a Zero Trust strategy.

## Ensure compliance

With local data centers around the world, personal data encrypted, user management of his data. **Cloudi-Fi makes sure the users comply with local regulations: Data privacy** (GDPR, CCPA, LGPD...) but also internet service provider laws.

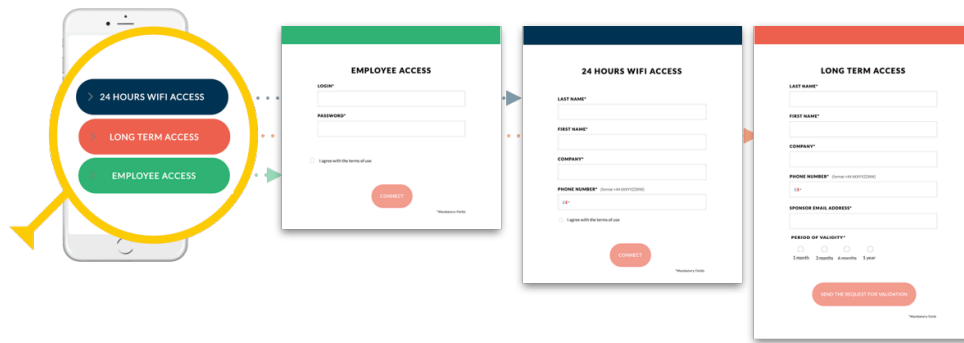
## Adopt a global solution

Cloudi-Fi can be deployed instantly, remotely, across the world regardless of the existing infrastructure. The architecture is **flexible and suited for SD-WAN environments with local internet breakouts**. The solution also interconnects with existing digital solutions.

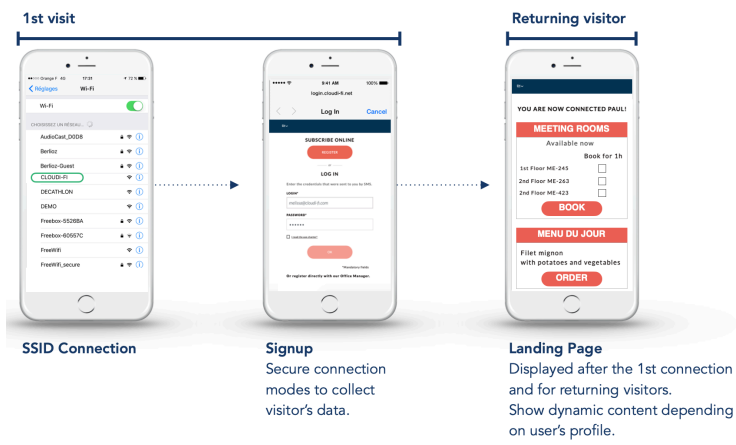


# APPLICATION

With **Corporate networks**, the solution uses the local Internet breakouts efficiently while removing the dependence to central solution.



The different types of users are **profiled** to propose and adapt a **compliant, secure and personalized** Wi-Fi access

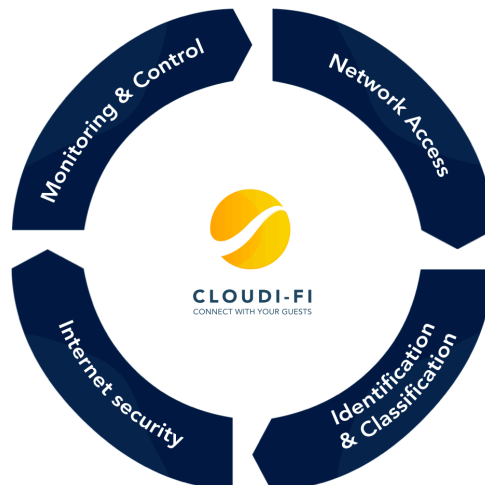


**Captive portal** pages can be leveraged to automate digital services on site.

With **IoT**, the solution accompanies the full IoT lifecycle by controlling the network access of the IoT assets, identifying and classifying the IoT into category, applying automated IoT security rules accordingly and monitoring the IoT behavior in real time for control and remediation.

IoT-specific security policies  
Continuous control with ML  
Automated remediation

Automated quarantine & whitelisting  
Automated policies by Cloudi-Fi's API w/ supported security solutions  
Security risk assessment

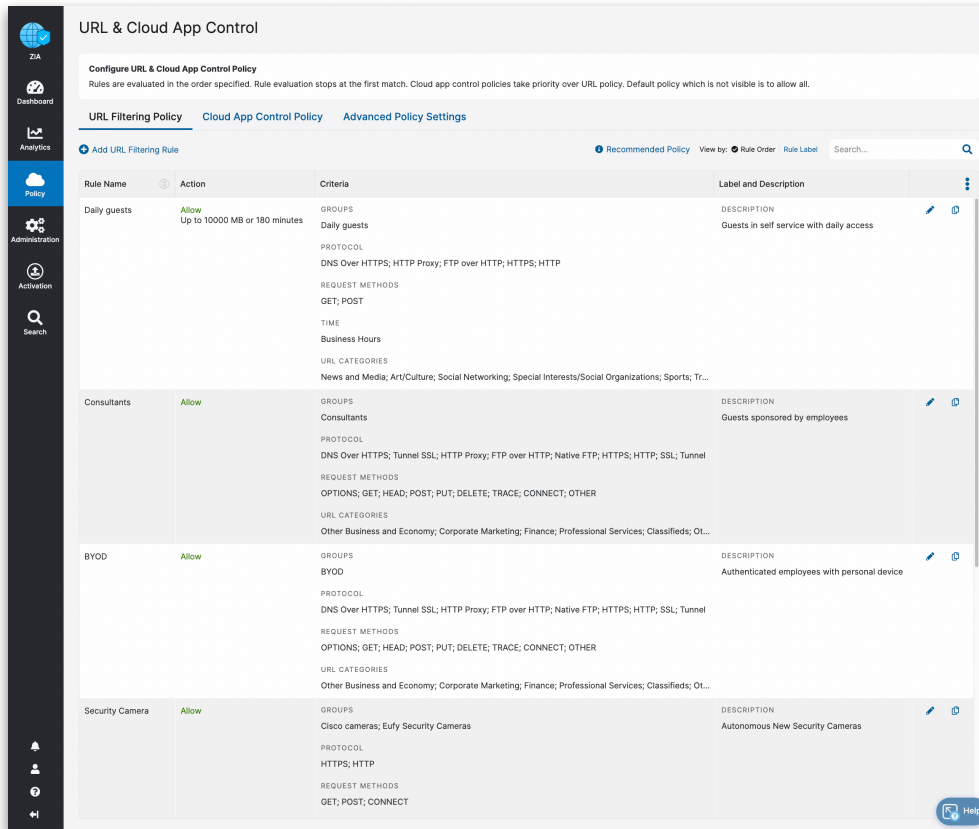


DHCP service in the cloud  
Uncover shadow devices  
Global IP address Management

Device fingerprinting  
IoT identification and classification  
Asset inventory

# ZSCALER AND CLOUDI-FI BENEFITS

One central management with delegated administration capabilities.



**URL & Cloud App Control**

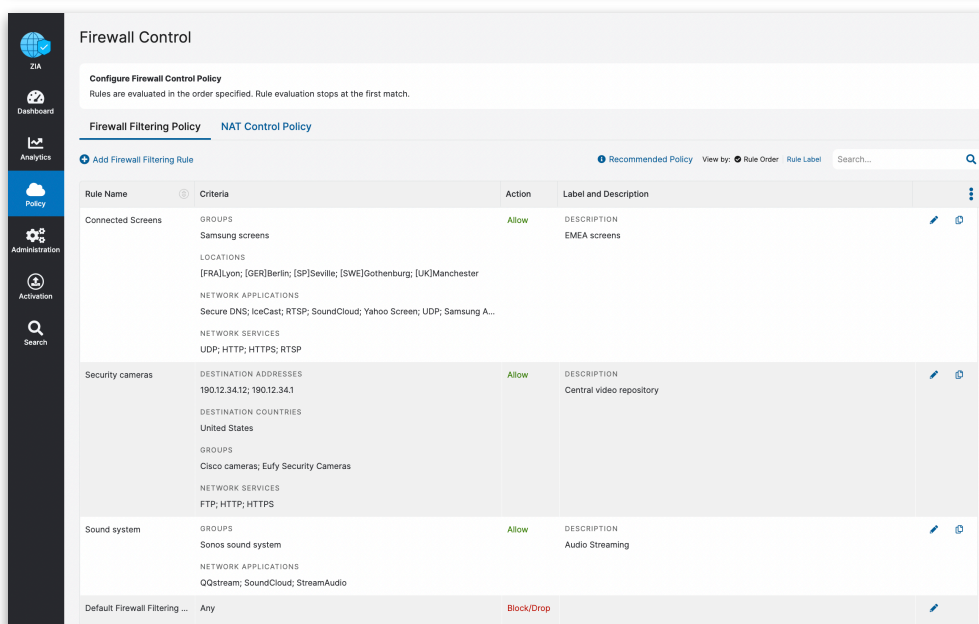
Configure URL & Cloud App Control Policy  
Rules are evaluated in the order specified. Rule evaluation stops at the first match. Cloud app control policies take priority over URL policy. Default policy which is not visible is to allow all.

URL Filtering Policy | Cloud App Control Policy | Advanced Policy Settings

+ Add URL Filtering Rule

Rule Name	Action	Criteria	Label and Description
Daily guests	Allow	<ul style="list-style-type: none"> <li>GROUPS: Daily guests</li> <li>PROTOCOL: DNS Over HTTPS; HTTP Proxy; FTP over HTTP; HTTPS; HTTP</li> <li>REQUEST METHODS: GET; POST</li> <li>TIME: Business Hours</li> <li>URL CATEGORIES: News and Media, Art/Culture; Social Networking; Special Interests/Social Organizations; Sports, Tr...</li> </ul>	<ul style="list-style-type: none"> <li>DESCRIPTION: Guests in self service with daily access</li> </ul>
Consultants	Allow	<ul style="list-style-type: none"> <li>GROUPS: Consultants</li> <li>PROTOCOL: DNS Over HTTPS; Tunnel SSL; HTTP Proxy; FTP over HTTP; Native FTP; HTTPS; HTTP; Tunnel</li> <li>REQUEST METHODS: OPTIONS; GET; HEAD; POST; PUT; DELETE; TRACE; CONNECT; OTHER</li> <li>URL CATEGORIES: Other Business and Economy; Corporate Marketing; Finance; Professional Services; Classifieds; Ot...</li> </ul>	<ul style="list-style-type: none"> <li>DESCRIPTION: Guests sponsored by employees</li> </ul>
BYOD	Allow	<ul style="list-style-type: none"> <li>GROUPS: BYOD</li> <li>PROTOCOL: DNS Over HTTPS; Tunnel SSL; HTTP Proxy; FTP over HTTP; Native FTP; HTTPS; HTTP; Tunnel</li> <li>REQUEST METHODS: OPTIONS; GET; HEAD; POST; PUT; DELETE; TRACE; CONNECT; OTHER</li> <li>URL CATEGORIES: Other Business and Economy; Corporate Marketing; Finance; Professional Services; Classifieds; Ot...</li> </ul>	<ul style="list-style-type: none"> <li>DESCRIPTION: Authenticated employees with personal device</li> </ul>
Security Camera	Allow	<ul style="list-style-type: none"> <li>GROUPS: Cisco cameras; Eufy Security Cameras</li> <li>PROTOCOL: HTTPS; HTTP</li> <li>REQUEST METHODS: GET; POST; CONNECT</li> </ul>	<ul style="list-style-type: none"> <li>DESCRIPTION: Autonomous New Security Cameras</li> </ul>

Cloudi-Fi solution provides user profiling and identification which allows Zscaler to define **specific security policies per user profile**.



**Firewall Control**

Configure Firewall Control Policy  
Rules are evaluated in the order specified. Rule evaluation stops at the first match.

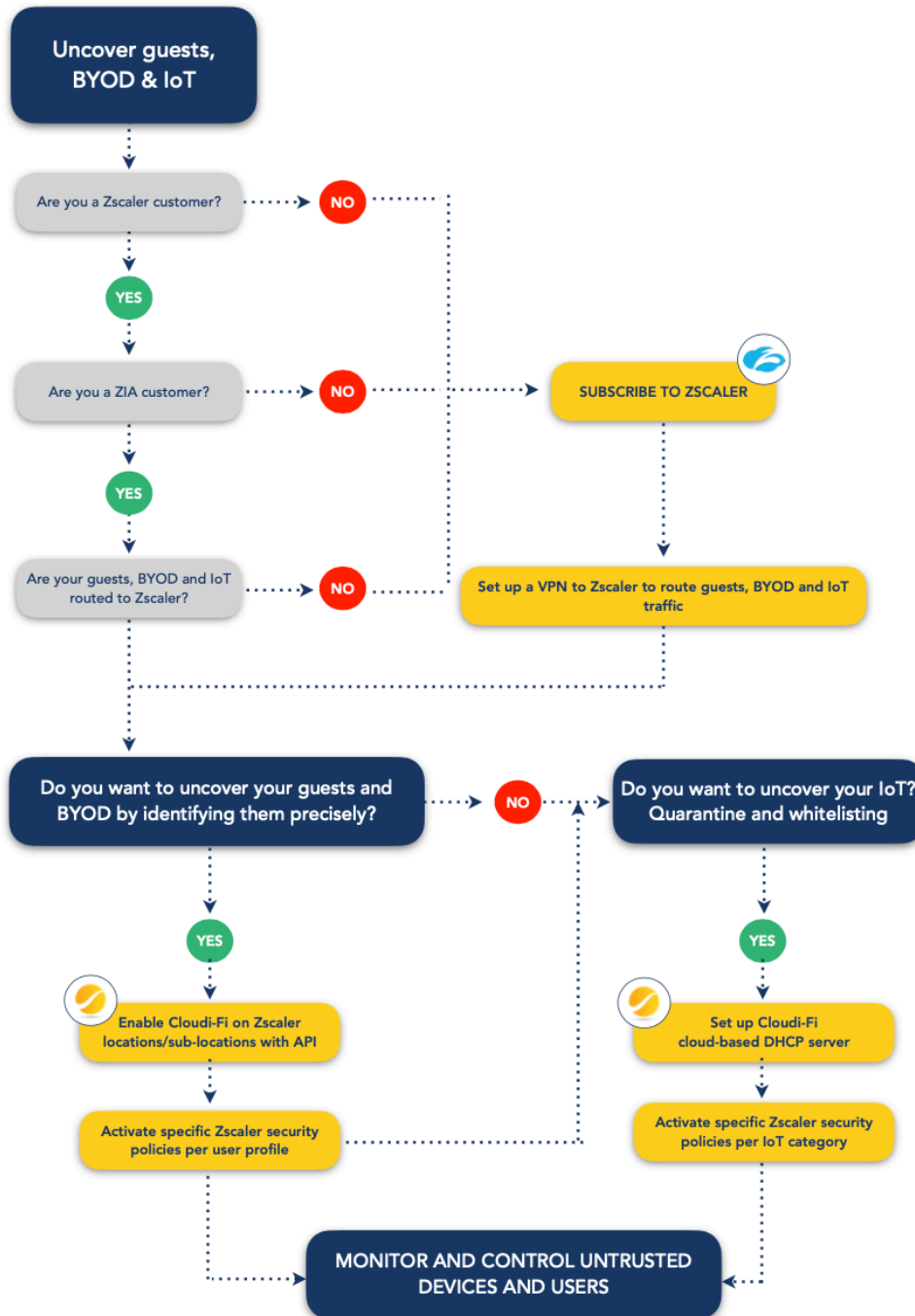
Firewall Filtering Policy | NAT Control Policy

+ Add Firewall Filtering Rule

Rule Name	Criteria	Action	Label and Description
Connected Screens	<ul style="list-style-type: none"> <li>GROUPS: Samsung screens</li> <li>LOCATIONS: [FRA]Lyon; [GER]Berlin; [SP]Seville; [SWE]Gothenburg; [UK]Manchester</li> <li>NETWORK APPLICATIONS: Secure DNS; IceCast; RTSP; SoundCloud; Yahoo Screen; UDP; Samsung A...</li> <li>NETWORK SERVICES: UDP; HTTP; HTTPS; RTSP</li> </ul>	Allow	<ul style="list-style-type: none"> <li>DESCRIPTION: EMEA screens</li> </ul>
Security cameras	<ul style="list-style-type: none"> <li>DESTINATION ADDRESSES: 190.12.34.12; 190.12.34.1</li> <li>DESTINATION COUNTRIES: United States</li> <li>GROUPS: Cisco cameras; Eufy Security Cameras</li> <li>NETWORK SERVICES: FTP; HTTP; HTTPS</li> </ul>	Allow	<ul style="list-style-type: none"> <li>DESCRIPTION: Central video repository</li> </ul>
Sound system	<ul style="list-style-type: none"> <li>GROUPS: Sonos sound system</li> <li>NETWORK APPLICATIONS: Qstream; SoundCloud; StreamAudio</li> </ul>	Allow	<ul style="list-style-type: none"> <li>DESCRIPTION: Audio Streaming</li> </ul>
Default Firewall Filtering ...	Any	Block/Drop	

Cloudi-Fi solution provides IoT identification and classification which allows Zscaler to define **specific security policies per IoT category**.

# ZSCALER AND CLOUDI-FI ELIGIBILITY



## SUMMARY

Zscaler offers security as a service through a unique zero trust platform. Combined with Cloudi-Fi services, enterprises gain visibility and control on Guests, BYOD and IoT use. The solution provides a full-featured compliant and secure solution.

To learn more about Zscaler and Cloudi-Fi solutions

Please visit

[Zscaler deployment](#)

[Zscaler Technology Partner page](#)

Contact us at [sales@cloudi-fi.com](mailto:sales@cloudi-fi.com)