CLOUDI-FI

FORTINET SOLUTION BRIEF

Cloud Identity and Policy Orchestration for Fortinet

Cloudi-Fi provides a cloud-based identity and access orchestration layer for guests, BYOD, and IoT, delivering real-time identity, authentication, and device context to enable consistent Zero Trust enforcement.

Challenges

Identity is the first prerequisite for controlling access and communication between users, devices, and systems. With strong identity management, organizations can enforce security policies to mitigate threats.

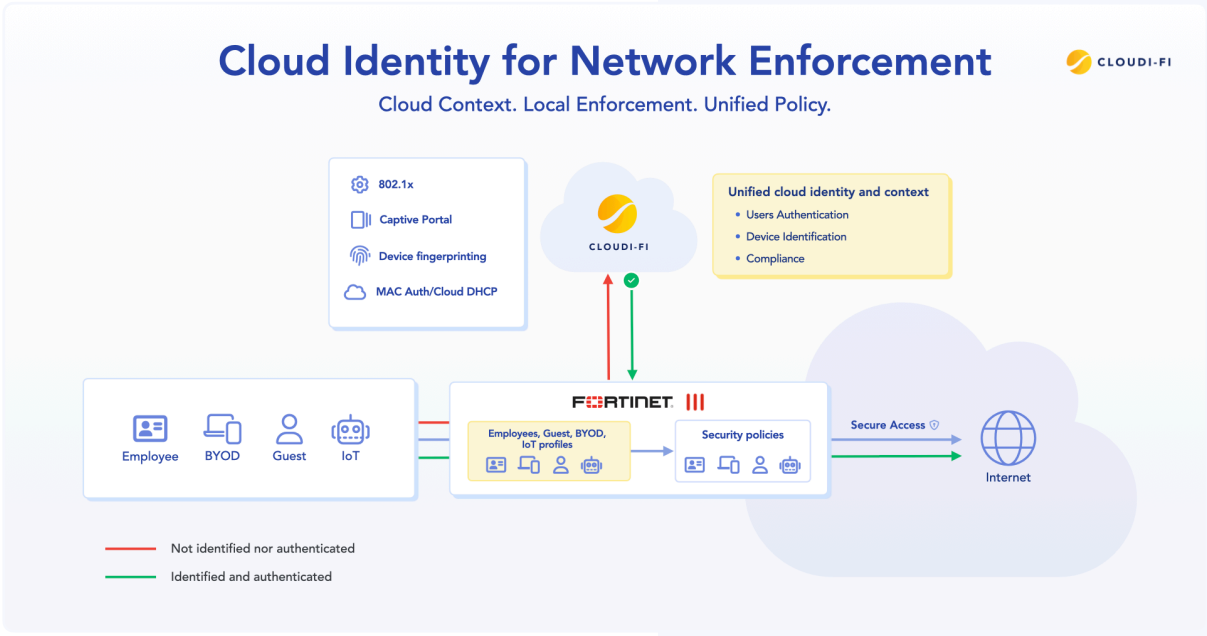
Enterprises face numerous challenges in identifying and controlling unmanaged devices and users: **Guests, BYOD, and IoT/OT**.

- **Absence of corporate credentials** for guests and external users makes identity verification challenging.
- **Onboarding and identifying IoT/OT** is complex as these devices lack native authentication mechanisms and user interfaces.
- **BYOD devices** connect outside of traditional directory and endpoint management frameworks.
- **Enforcing least-privilege** access across heterogeneous environments remains complex
- **Meeting regional data privacy** and consent requirements (e.g., GDPR) requires dedicated onboarding and traceability mechanisms.

These gaps create blind spots at the network edge, where Zero Trust enforcement often breaks onboarding and traceability mechanisms.

Benefits

- ✓ Extend Zero Trust identity and context to unmanaged users and devices at the network edge
- ✓ Seamlessly onboard, identify, and classify guests, BYOD, and IoT at scale
- ✓ Enforce least-privilege access policies through FortiGate and Fortinet Security Fabric
- ✓ Cloud-based, plug-and-play deployment with Fortinet infrastructures
- ✓ Centralized visibility and policy orchestration through a unified management layer
- ✓ Globally compliant identity and access framework



Overview

Unified identity, policy, and access orchestration

The platform simplifies network access and device management across all users and devices—managed corporate devices, employees with BYOD, guests, and IoT. By integrating captive portal, 802.1X, and DHCP fingerprinting, it orchestrates Zero Trust network access, ensuring identity and authentication are validated before network access is granted.

Global data privacy compliance

Granular Zero Trust access policies enforce strict user and device authentication with least privilege access, while integrated privacy and security controls ensure regulatory compliance.

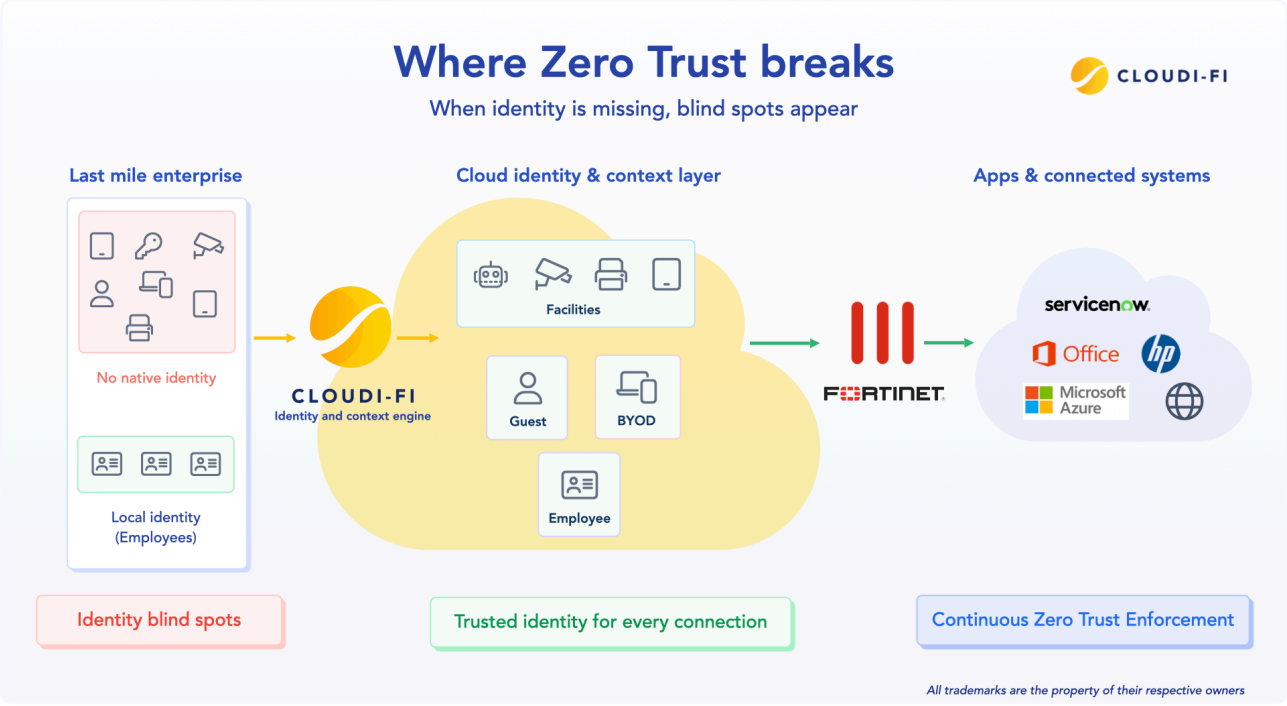
Scalability and plug-and-play integration

As a cloud-native platform, Cloudi-Fi integrates seamlessly with Fortinet infrastructures through APIs and native workflows, enabling rapid multi-site deployment and a consistent security posture.

Testimonial

"Modern cybersecurity requires real-time flexibility and granular control over access and identity. By combining Fortinet enforcement with Cloudi-Fi's real-time identity and context orchestration, organizations can implement scalable, policy-based Zero Trust across distributed environments."

Alain Sanchez
Fortinet EMEA FCISO



https://www.cloudi-fi.com/platform/technology-integration-partners/fortinet
Contact: sales@cloudi-fi.com

CLOUDI-FI