PANGOLIN

Stars 20k

Zero Trust Remote Access

for IoT, edge, and infrastructure.

• Connected

Secure VPN

Web Access

SSH and RDP

Identity Aware

contact@pangolin.net
www.pangolin.net

Web Access & Client Access

Securely reach edge dashboards directly from any web browser using our identity-aware reverse proxy. When direct VPN-like connectivity is required for system tasks, switch to the Pangolin Client to establish high-performance, peer-to-peer tunnels while utilizing the same identity-based controls.

Rapid Fleet-Scale Deployment

Scale from ten sites to ten thousand without increasing operational overhead. Our declarative provisioning allows you to roll out new hardware instantly using automated YAML templates and secure "golden image" workflows. Leverage flexible metadata tagging and resource labeling to organize, sort, and manage massive device fleets with ease.

Easy Network Segmentation

Protect critical infrastructure by eliminating lateral movement between sensitive installations. Our hub-and-spoke architecture ensures that every edge site remains isolated, eliminating the management overhead and security risks of mesh sprawl by granting users access only to the specific resources they are authorized to reach.

Monitoring & Real-Time Alerting

Connectivity is only valuable when your equipment is online. Pangolin provides integrated uptime tracking and instant notifications via email, webhook, and custom integrations like Slack or PagerDuty, ensuring you are the first to know if a remote resource or site becomes unreachable.

Open-Source and Enterprise Ready

- All code is 100% open-source.
- SOC-2 Type 2 and ISO 27001 certified.
- Highly available with SLA backed support.
- Used and trusted by thousands of organizations.

ISO 27001

AICPA SOC2 TYPE 2

PANGOLIN

Fine-Grained Resource Access

Pangolin moves beyond broad network-layer VPNs by abstracting your infrastructure into logical Sites and specific Resources. Instead of granting a user access to an entire subnet, you define exactly which applications, IPs, ports, or hostnames a role can interact with.

- **Resource-Level Granularity:** Grant access to specific assets.
- **Zero-Trust Sessions:** Authenticate every connection attempt.
- **Identity-Driven RBAC:** Integrate SSO via Entra ID or Google.
- **Compliance-Ready Logs:** Audit access attempts to everything.

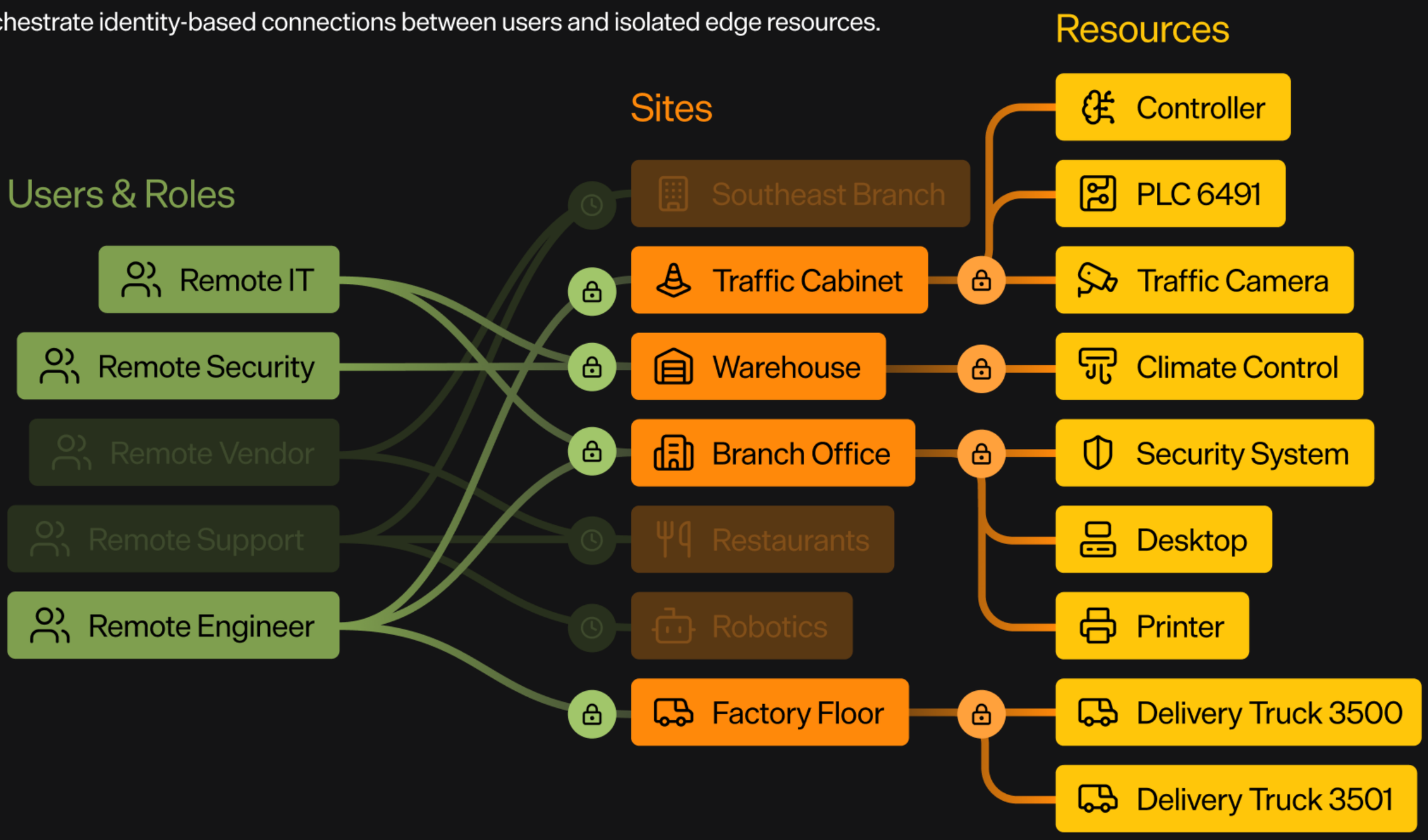
Flexible Connectivity Architecture

Engineered for resource-constrained IoT gateways and headless hardware, our userspace connector can be deployed instantly as a standalone binary or container. It orchestrates encrypted sessions that dynamically adapt to your network environment, providing stable connectivity over unstable LTE, 5G, or satellite links.

- **Light Connector:** Runs on Linux, Windows, or Darwin gateways.
- **High-Performance P2P:** Direct WireGuard® tunnels as needed.
- **Seamless NAT Traversal:** Bypass CGNAT and firewalls.
- **Scale:** Hub-and-spoke architecture to eliminate mesh sprawl.

How it Works

Orchestrate identity-based connections between users and isolated edge resources.



The diagram illustrates the Pangolin deployment architecture, where a single connector is installed at the edge to establish an isolated Site. Rather than installing software on every asset, the site-level connector proxies connections to any device on its local network, transforming them into specific Resources. Users connect to these resources based on least-privilege access, utilizing friendly DNS aliases like plc.site.internal to reach authorized hardware without needing to manage complex IP routing.

ISO 27001 · AICPA SOC2 TYPE 2