WHO WE ARE

INTELLIGENTLY SIMPLE DESIGN

One SSID automatically places devices into their correct secure VLAN

Simple web dashboards for staff and users that can be quickly learned

FLEXIBLE OPERATIONS

Provide private VLANs and unique bandwidth packages or offer standard tiers

SECURITY & RESILIENCY

No need to activate specific data ports; devices can securely connect to any port

OUR APPROACH

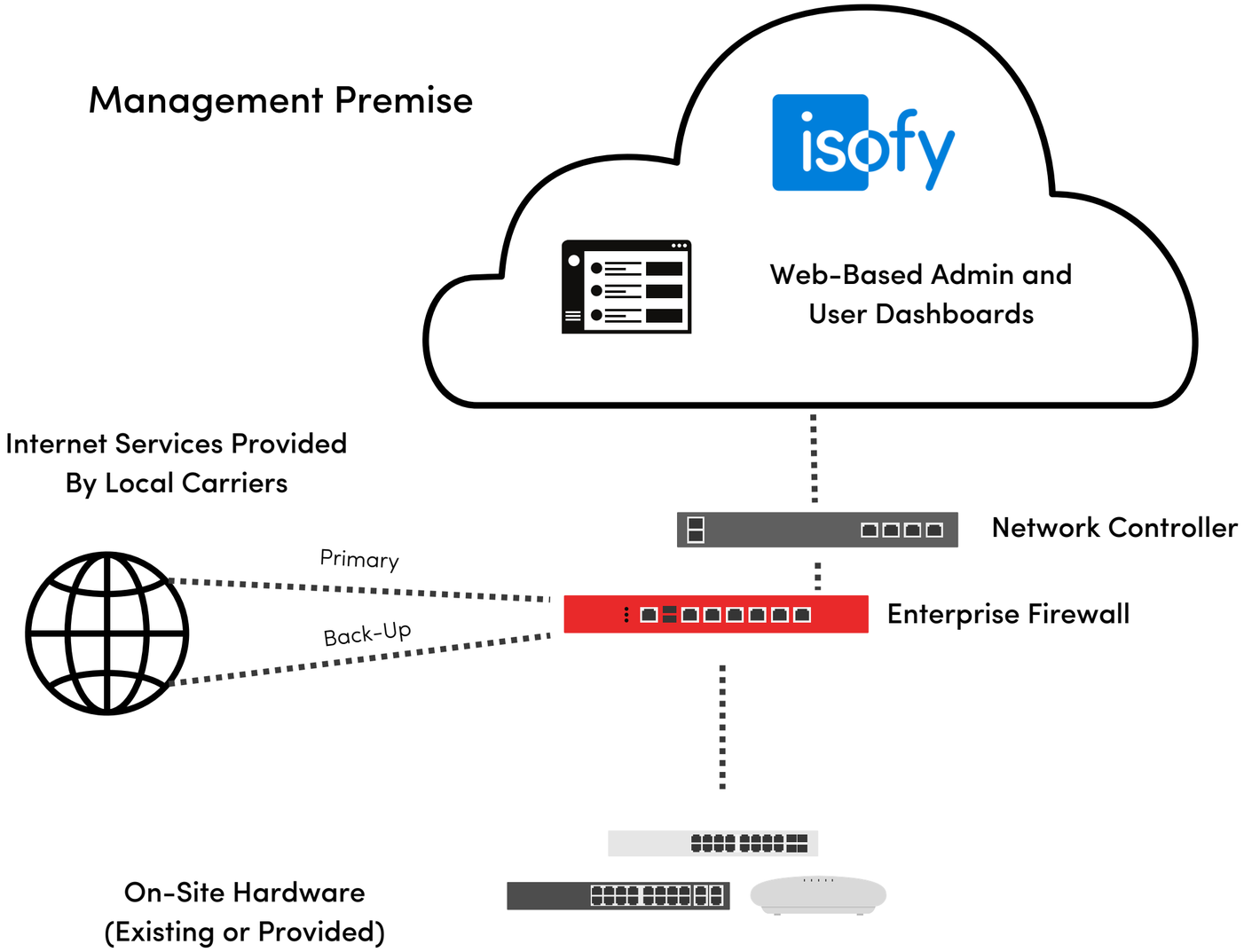
Delivering a world-class network management platform instead of an end-to-end operating solution, providing focused excellence and reducing your business risk

FOUNDED IN 2019
BUILT BY CYBER SECURITY FIRM
ACQUIRED IN 2022 BY PORTSIDE TECHNOLOGY
NOW LED BY EXPERIENCED COMMERCIAL REAL ESTATE TECHNOLOGISTS

Active sites across the United States, Canada, Puerto Rico, and Australia

HQ in Charleston, SC

HOW WE'RE DIFFERENT



Management powered by on-site devices without risk of a central data center failure

Accurate geo-location services with local internet service providers

Provide secure network access codes to large groups and events to streamline connectivity

Integrate with your workspace management platform to simplify onboarding & removal

Negotiate directly with local internet carriers and procure your own circuits

Use your existing compatible equipment and reduce capital expense

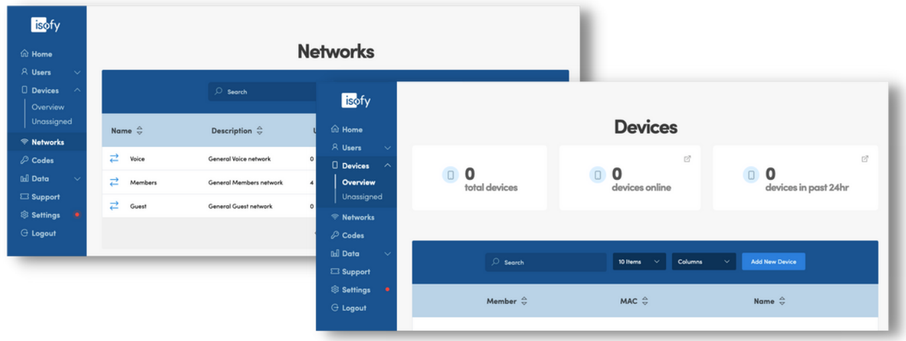
PLATFORM OVERVIEW

A SOFTWARE-FIRST COMPANY

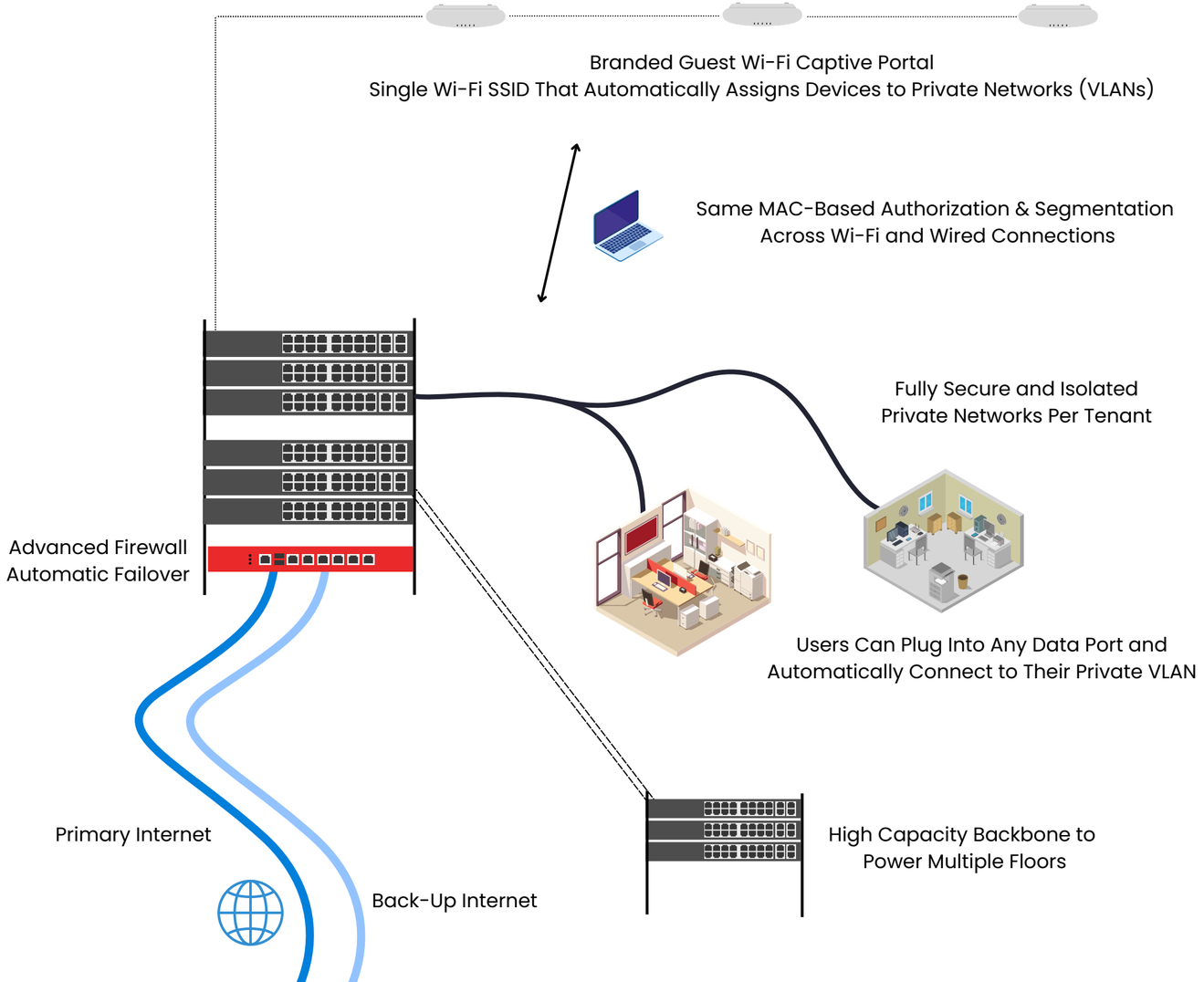
We deliver a world-class network management platform with plug-ins for some of the most common enterprise-grade networking equipment in the industry.

HOW WE HELP

Provision users, authorize devices, create private networks, and assign bandwidth tiers in real-time with a simple web-based dashboard. Or automate these tasks with an integration with your workspace management software.



TYPICAL SYSTEM OVERVIEW



PLATFORM SECURITY DETAILS

AUTHENTICATION & USER ACCESS

- Access to the network is authenticated by device MAC address.
- Authenticated devices are linked to a user, making it easy to control both user- and device-level access on the network.
- Data ports are also configured in this way, making it easy and reliable for staff to ensure that every port is secured, without the risk of a possible security hole.
- Access to the isofy Dashboard software is authenticated by secure username and password
- If user-level access needs to be removed, then simply mark that user inactive, and all of the user's devices will be disconnected from the network and blocked from accessing the local network or internet connection.

ROLE-BASED PERMISSIONS & NETWORK SEGMENTATION

- Role-based permissions are implemented for every user on the network to limit access only to approved resources.
- isofy excels at role-based permissions by not only configuring users' access but also completely and automatically isolating them from each other using VLANs. With isofy, role-based permissions are automatically supplemented by role-based network segmentation.
- Each device is authorized to access the VLAN of the assigned user. Devices are attached to users, and users are attached to clients (VLANs), creating a secure environment with a granular permission structure.
- Network access is restricted to the assigned VLAN. Attempting to access a device on another VLAN is blocked by the firewall. The only exception to this rule is made for communal resources such as printers or screen share devices.
- Within the Dashboard, easily view which user owns each device that has access to your network and is using your network resources.
- Automatically isolate groups of people, without having to manually track each device, which could lead to a configuration oversight and a security hole.

FIREWALL

- isofy maintains a properly configured and up-to-date firewall on all isofy networks.
- The firewall filters all access by MAC address.
- isofy documents all firewall configurations internally and regularly reviews them to ensure that they are functioning as intended.

HIPAA COMPLIANT

PCI

Secure and compliant infrastructure that allows your customers to meet organizational and industry-specific compliance requirements.

NETWORK EQUIPMENT AUTHENTICATION

- Each piece of network equipment is individually added to the platform. The network access controller will not allow authentication requests from network equipment that has not been added to the platform. This prevents untrusted equipment or devices from being added and authenticating devices on the network, or spoofing data.

AUDIT LOGS

- All actions on the network are automatically logged, and logs are retained for a length of 6 years.
- Logs are tied to both individual users and individual MAC addresses so actions can be traced to specific devices.
- Device tracking allows seeing when specific users or specific devices access the network, both historically and in real-time.

ENCRYPTION

- All data passing through the isofy software is encrypted via SSH and TLS connections using AES-256 encryption.
- WPA3 authentication is enforced by all Wi-Fi devices provided by isofy for the network.

GUEST NETWORK

- Unauthenticated devices are segmented into a guest VLAN that is completely isolated, with no local network access or internet access. Devices must be approved via MAC authentication to move from the guest VLAN into a VLAN that has network access.