Console & IP Dedicated OOBM Networks

FRNOG 39

Automatic Provisioning with IP and Console Access on a Dedicated Out-of-Band Management Network

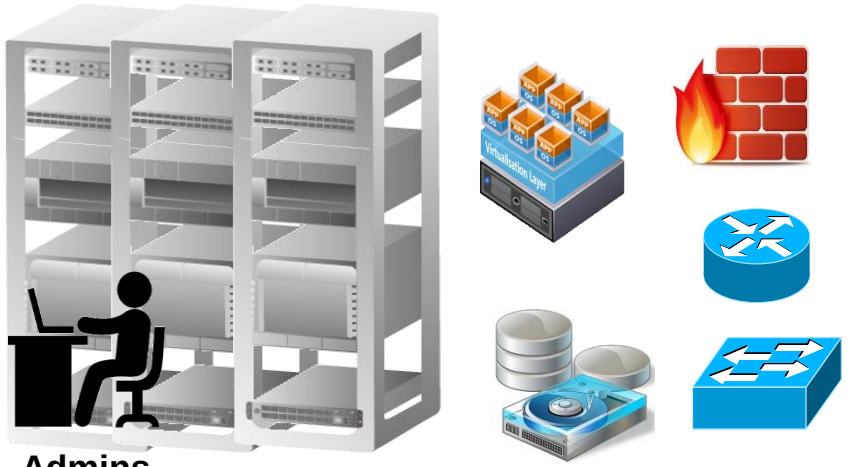
Alan Barnett <alan.barnett@opengear.com>

EMEA SE Manager, Opengear

Content

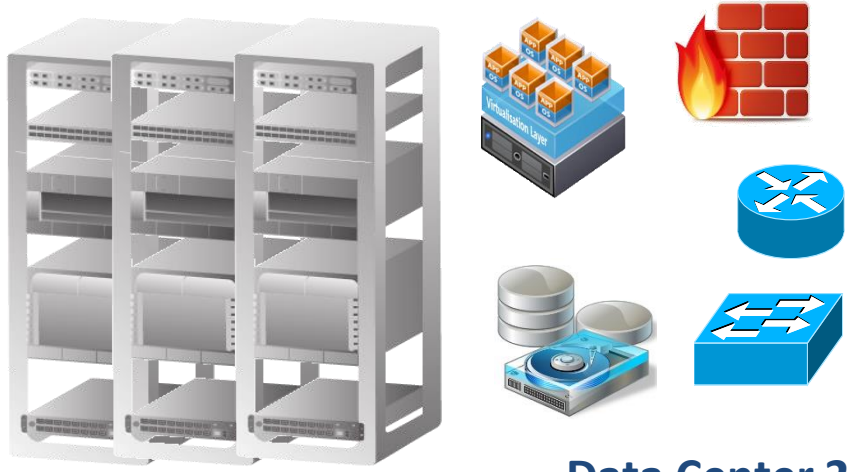
Common environment

Data Center 1



Admins

Data Center 2



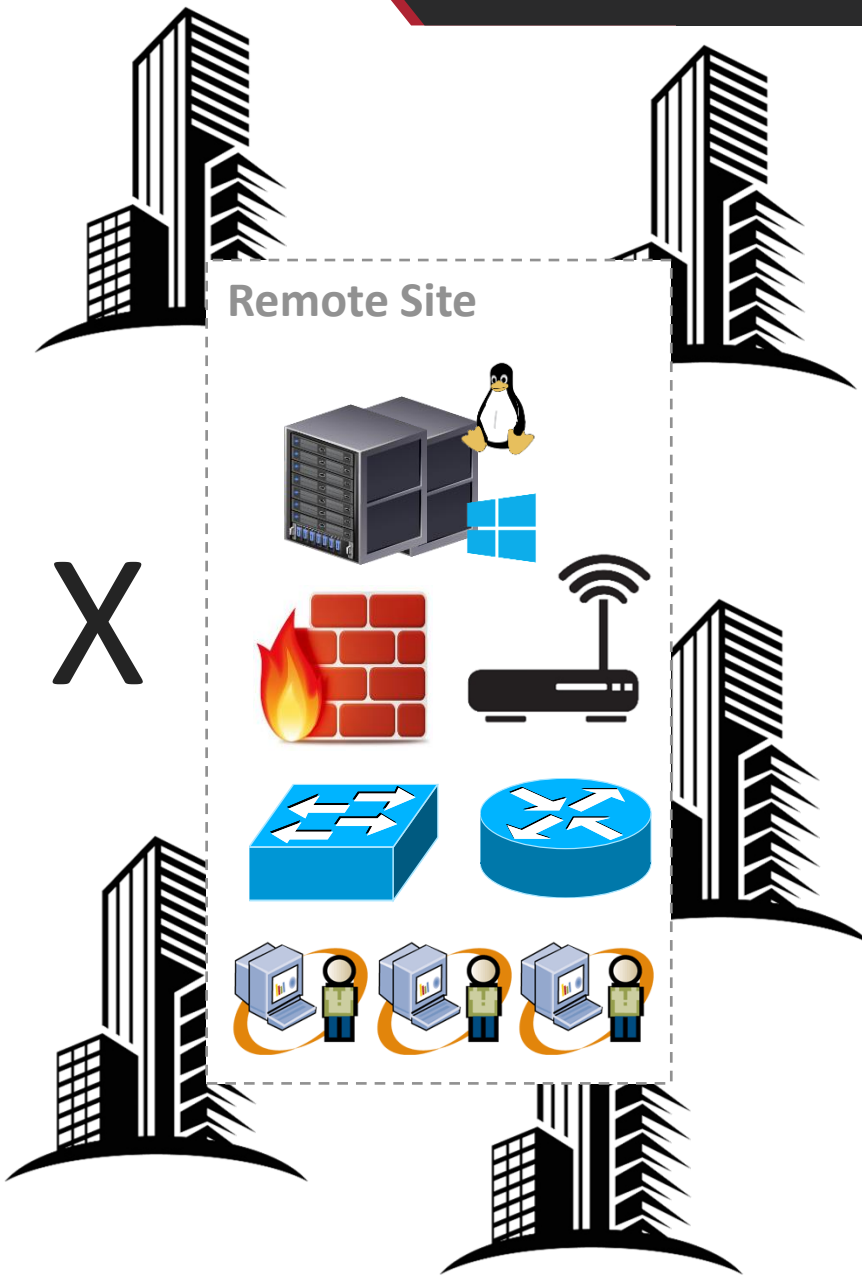
Public Internet

MPLS

Carrier Ethernet

X

Remote Site



Challenges

Outages can be very costly for enterprises

High Availability only solves part of the problem

Skilled professionals can’t be omnipresent

Remote work is challenging

Skills Gap and Talent Shortage

Security has never been more important

Legacy System Maintenance is a challenge

IT is becoming more complex with many new technologies

Operational teams struggle to maintain efficiency in when technologies and threats are evolving

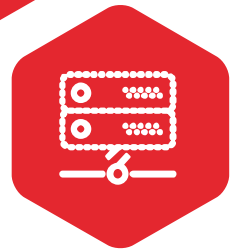
Hybrid work is here to stay

Business criticality of network increasing and IT budget for networking decreasing driving automation

Traffic patterns fluctuated

Rarely used apps are now everyday apps

More Hardware to manage remotely

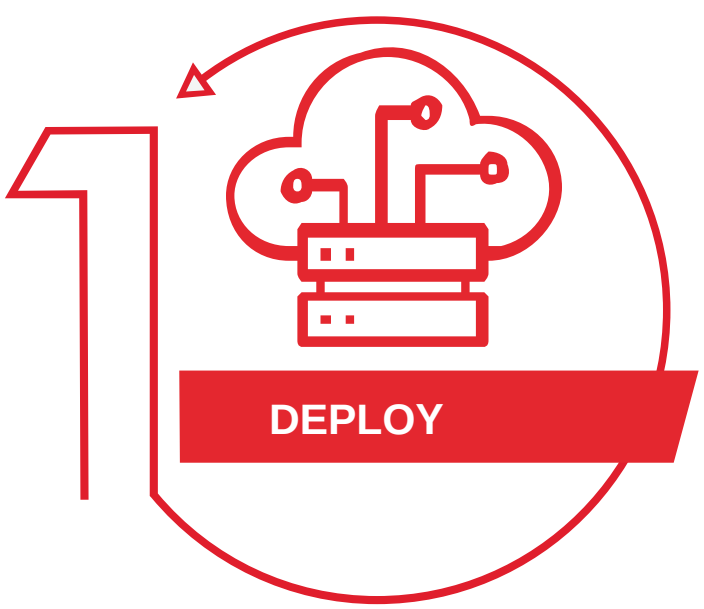


Need for more Agile and Resilient Networks

The world went through a seismic shift
Networks need to be more resilient and respond to technology needs of the business

DEPLOY

Serving on the First day

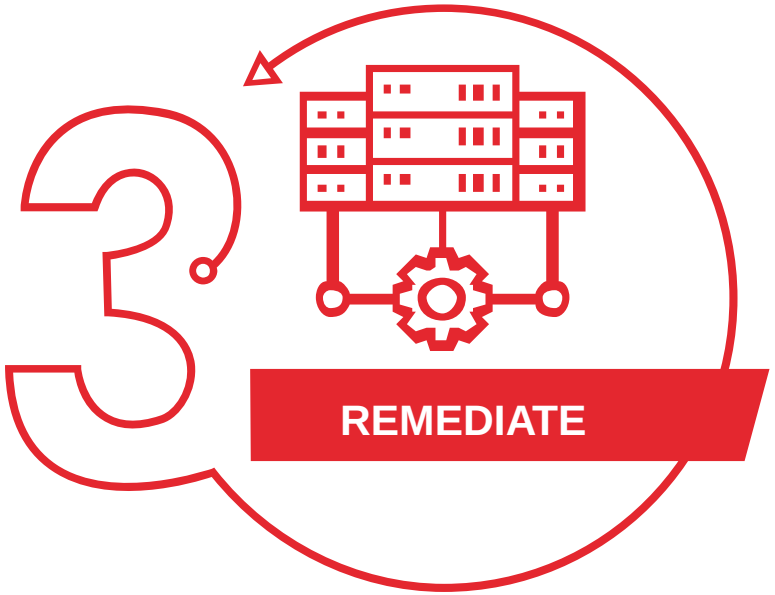


MANAGE

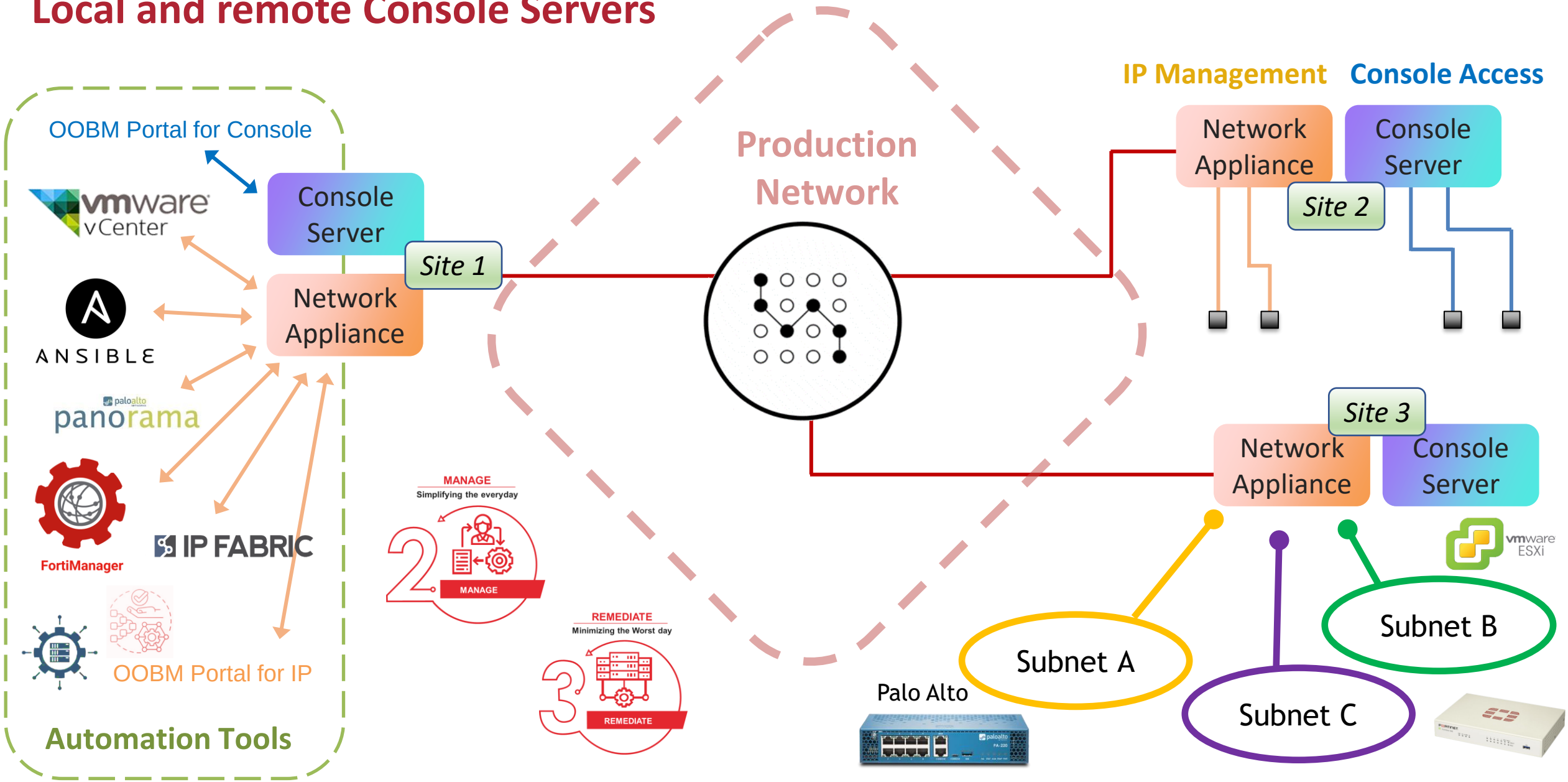
Simplifying the everyday

REMEDIATE

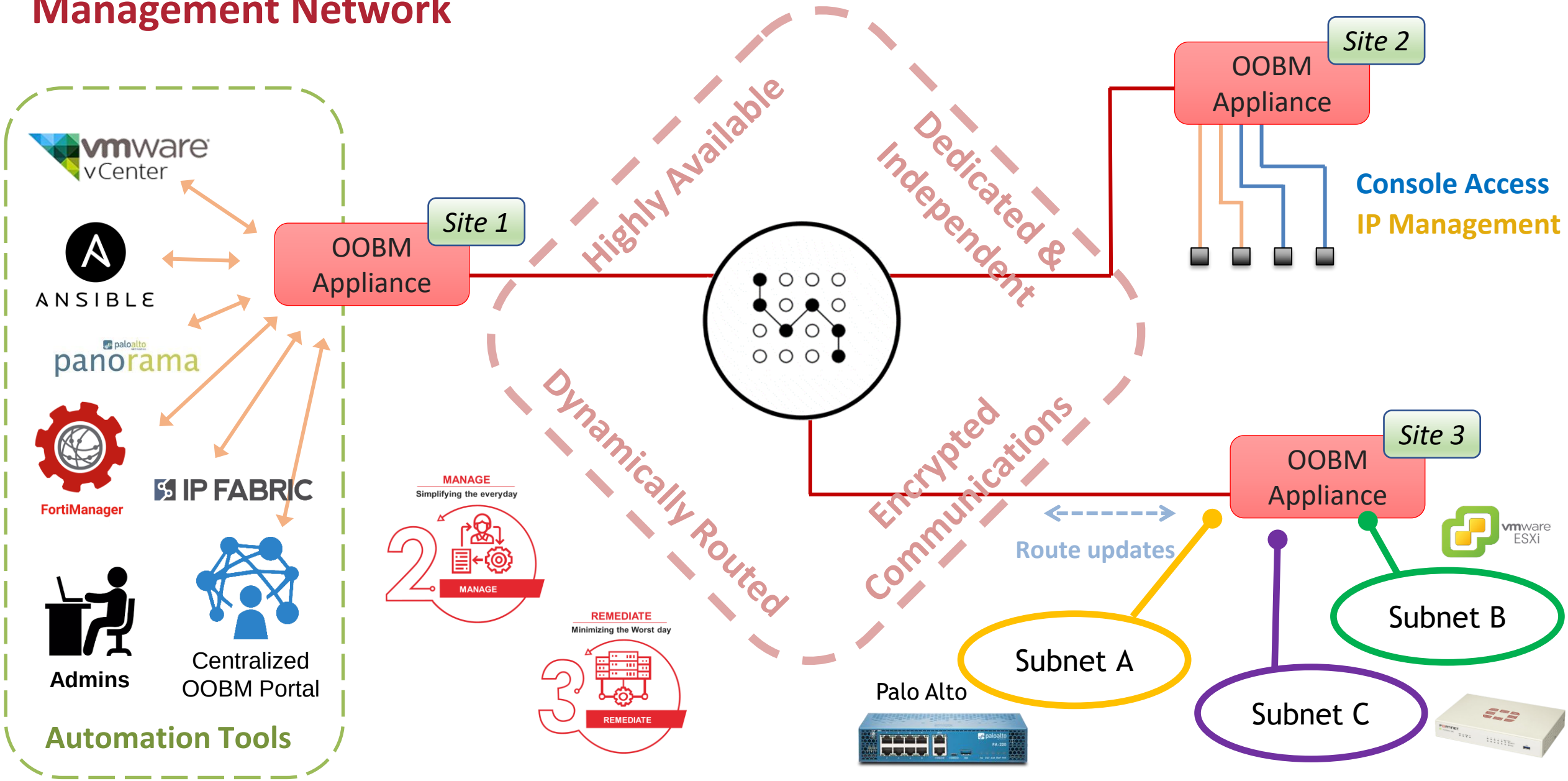
Minimizing the Worst day



Mixture of In-Band IP Management with Local and remote Console Servers



Dedicated Console & IP Out-of-Band (OOB) Management Network



Secure, Reliable and Centralized, Remote Access via the OOB Network

Console & IP Dedicated OOBM Networks

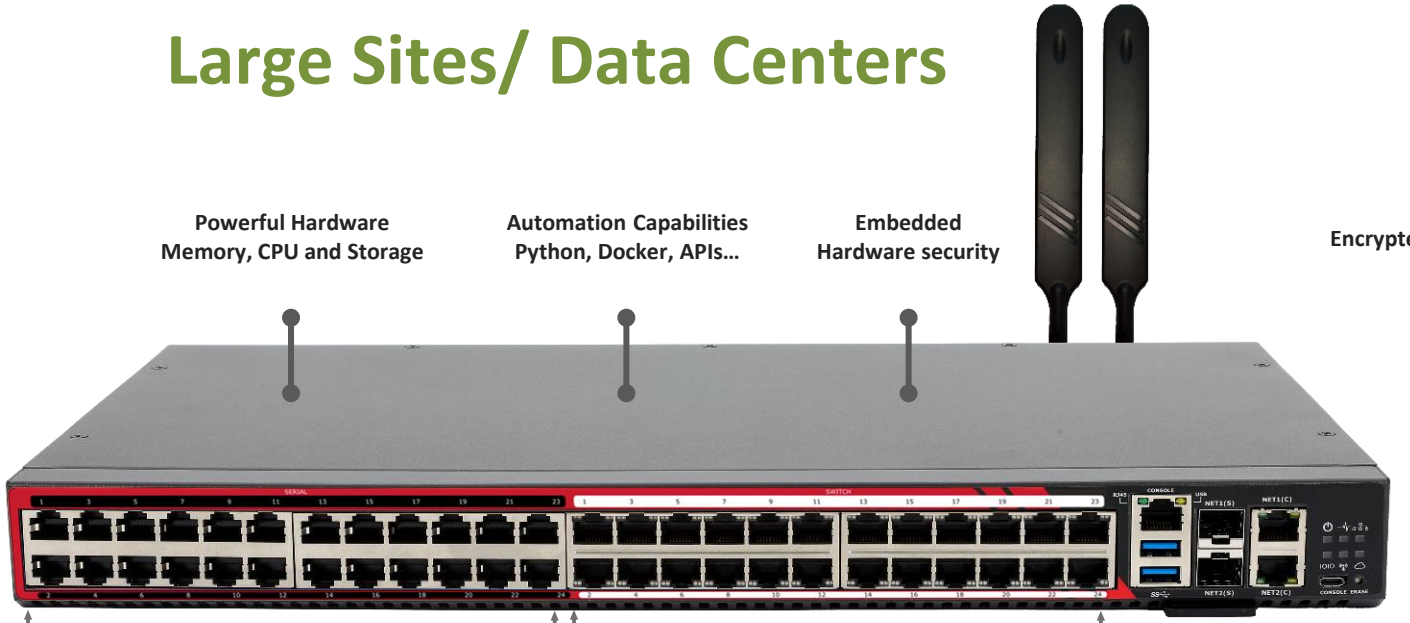
Large Sites/ Data Centers

Powerful Hardware
Memory, CPU and Storage

Automation Capabilities
Python, Docker, APIs…

Embedded
Hardware security

Encrypted Storage



24x Serial console ports
Software selectable pinout, no adapters needed

24x 1Gb Ethernet switch ports
VLAN and dynamic routing support

SFP | RJ45 Gbe uplinks

SIM slots

4G/5G Antenna connections

USB serial console ports

Dual Power AC or DC

Smaller Sites

8 Serial ports
X2 pinout

8 port 1GbE switch
VLAN and routing

Deployment Considerations for OOBM Networks

Out of Band Management Networks need

- Availability
- Confidentiality
- Authenticity
- Integrity
- Traceability & Auditing

Network topology with redundant pathways

Failover to alternative media capabilities

Load Balancers and Highly Available servers for critical services

Hardware with long MTBF, Redundant Power supply and hot swap

Console and IP Security layer

Secured encryption protocols (IPSec, OpenVPN, Wireguard, SSH, HTTPS…)

RBAC policies for granular access management

Integration with external authentication methods (Radius, TACACS, LDAP, MFA)

Integrated firewalling mechanisms

Brute force and DDOS protection

Vulnerability management, code auditing and PEN testing by manufacturers

Disk encryption for locally stored files

Audit trails for access to all components of the OOB network

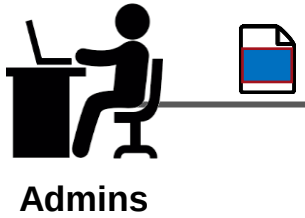
Traceability for Console and IP access

Ability to send traces (logs, traps, files) to a compliance logging system

Auditing by forward logs to meet regulatory requirements

Secure Remote Provisioning of Devices

Manual



OOBM Appliance

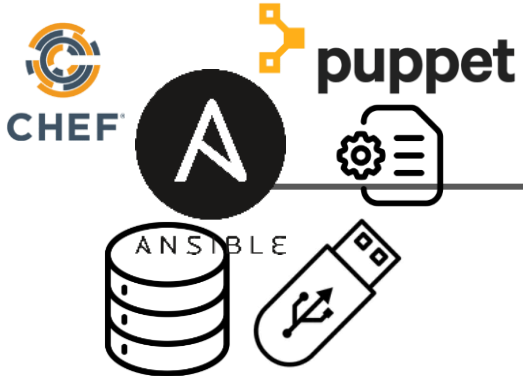
Console Access

IP Management

Semi Automated

Ansible, Puppet, Chef

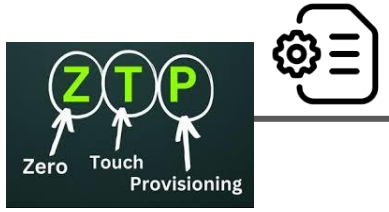
Storage (local & USB)



OOBM Appliance

Fully Automated

ZTP



OOBM Appliance

Hybrid configuration from OOBM Node (Console & IP)

Secure Remote Provisioning – Fully Automated over LAN

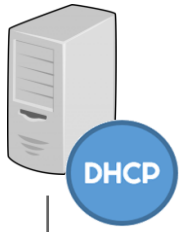
Key Components

DHCP server for IP address assignment
TFTP server for storing device configurations
Bootstrap configuration file (e.g. DHCP option 67)
Automated configuration scripts or templates
Revision control with roll-back for configuration files

Workflow

1. Device boots and requests an IP address via DHCP
2. Local DHCP server responds with the IP address and the location of the configuration file (TFTP server)
3. Device downloads the configuration file and applies it
4. Automated scripts or templates execute additional configurations as needed
5. Device becomes operational without manual intervention

Secure Remote Provisioning – LAN



DHCP Request

DHCP Response
(IP Address, DNS Server, options…)

Bootstrap Data Request | Configuration Script or File

Data Received

Configuration Applied

DEPLOY
Serving on the First day
DEPLOY

Secure Remote Provisioning – Fully Automated over WAN

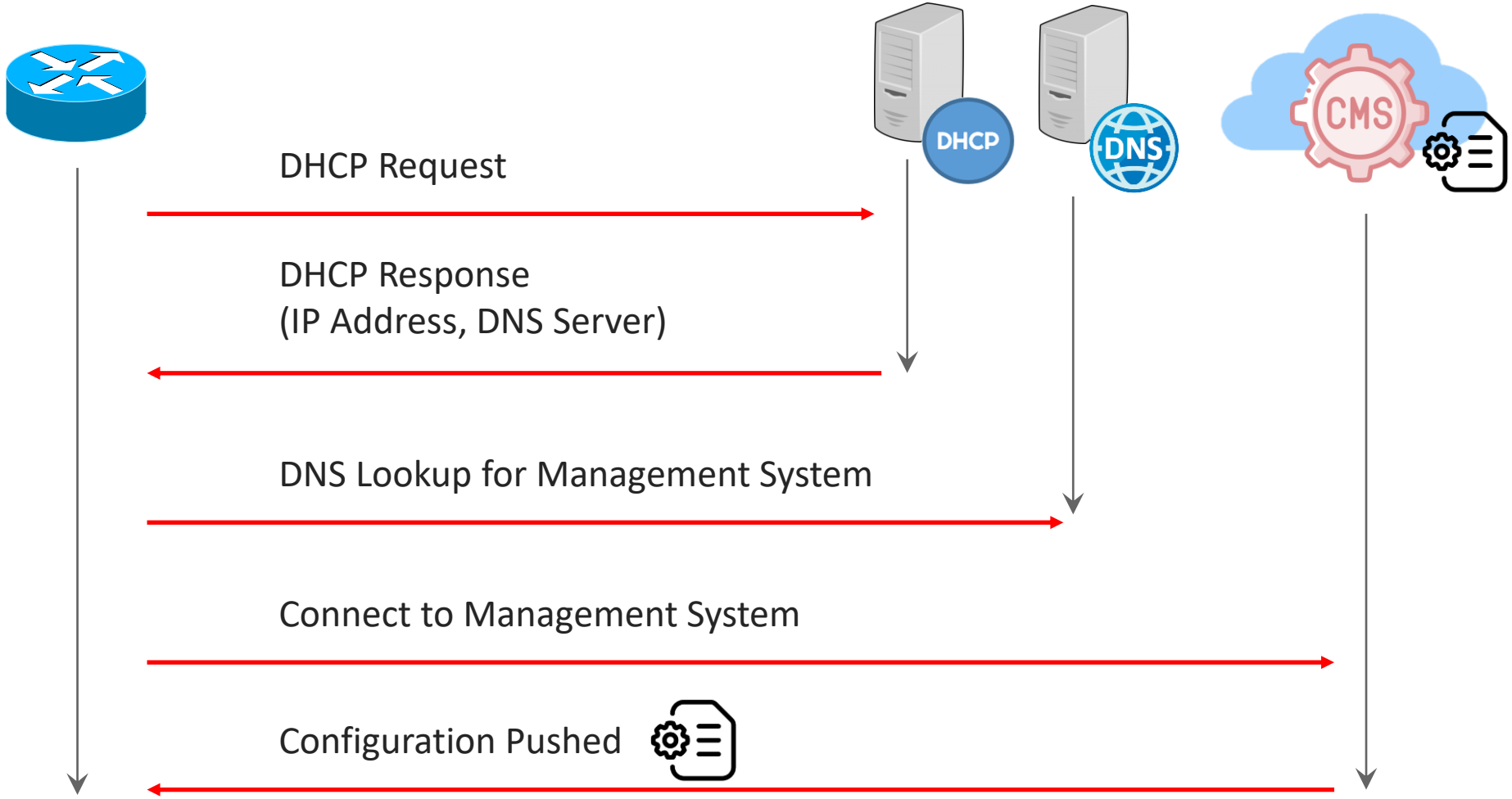
Key Components

Centralized provisioning server or cloud-based platform
Secure communication protocols (e.g. HTTPS, SSH)
Secure authentication mechanisms (e.g. certificates, tokens)
Automated configuration scripts or templates
Revision control with roll-back for configuration files

Workflow

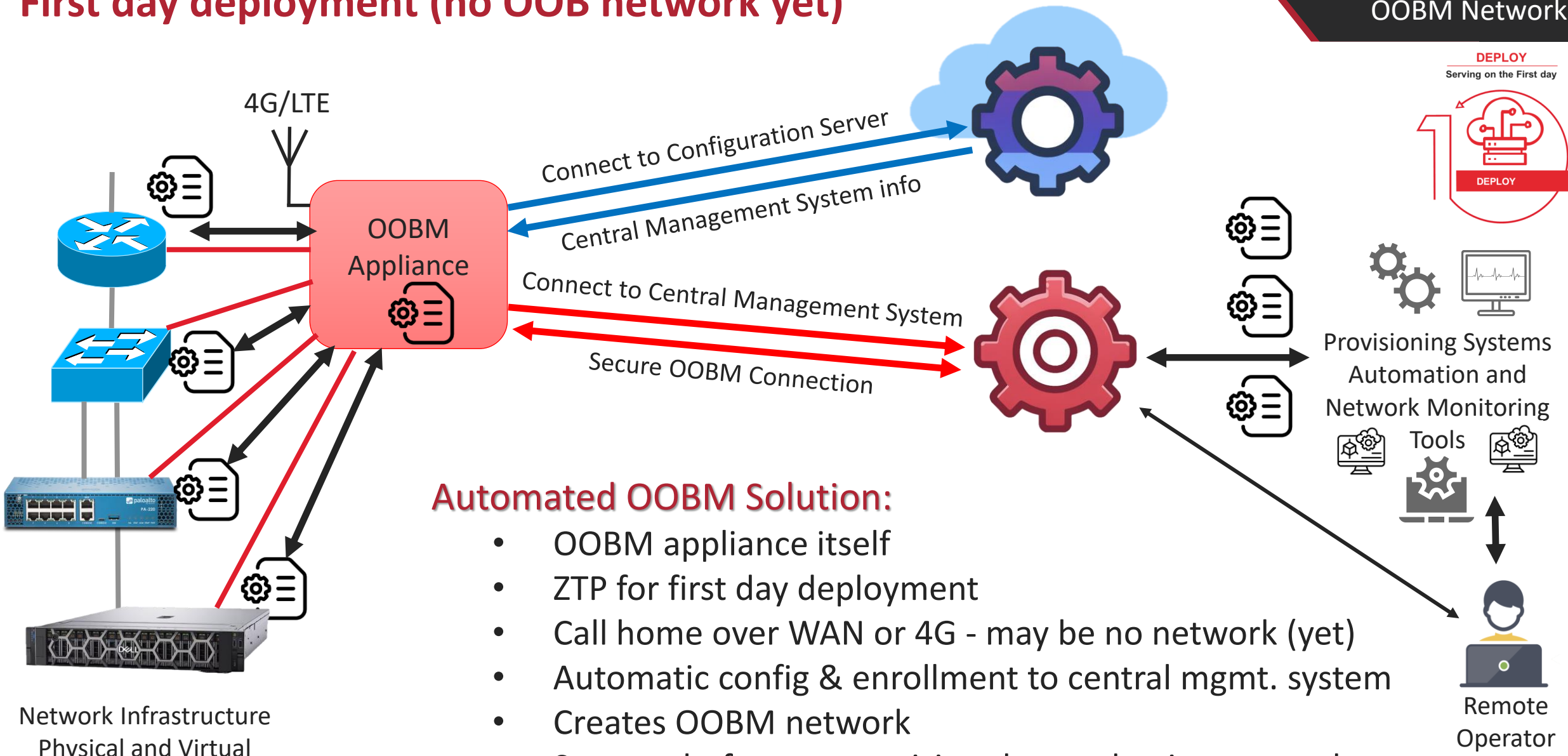
1. Device boots and establishes an internet connection
2. Device communicates with the centralized provisioning server or cloud platform
3. Provisioning server validates device identity and credentials.
4. Provisioning server delivers device-specific configuration and firmware updates over the internet
5. Device applies the configuration and becomes operational without manual intervention

Secure Remote Provisioning – WAN



DEPLOY
Serving on the First day

First day deployment (no OOB network yet)



Automated OOBM Solution:

- OOBM appliance itself
- ZTP for first day deployment
- Call home over WAN or 4G - may be no network (yet)
- Automatic config & enrollment to central mgmt. system
- Creates OOBM network
- Secure platform to provision the production network

Thank You

Opengear contacts in France

Thomas Mercon: <thomas.mercon@opengear.com>

Romain Pia: <romain.pia@opengear.com>

Julien Orsolini: <julien.orsolini@opengear.com>