

CISCO *Live!*



GO BEYOND

#CiscoLive



The bridge to possible

Securing the Network's Backbone

using 3rd Gen Out-of-Band (OOB) Isolated Management Infrastructure

Rene Neumann

Director of Solution Engineering
ZPE Systems, Inc.

CISCO *Live!*

#CiscoLive

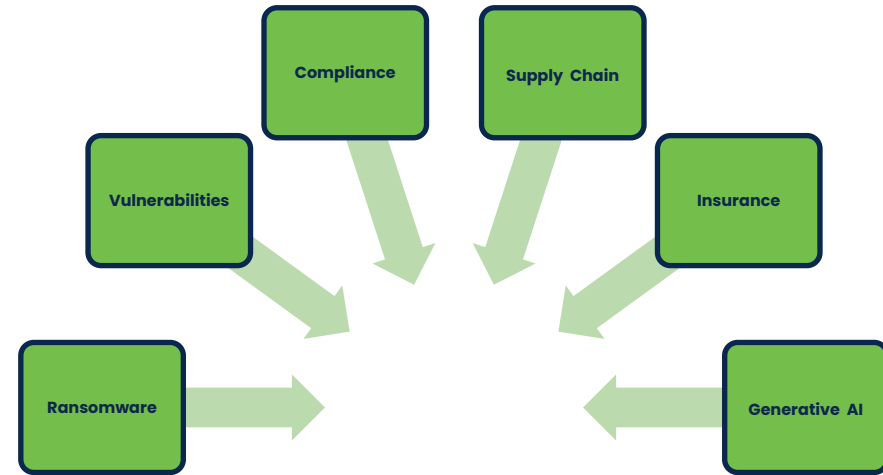
A decorative graphic in the bottom right corner consisting of a series of overlapping, rounded, teardrop-like shapes. The colors transition from dark red on the left to bright yellow on the right, creating a vibrant, abstract background element.



Agenda

- Security Trends in 2024
- Resilience and Isolated Management Infrastructure
- Isolated Management Infrastructure
- Traditional Deployments

Security Trends 2024



CISA
CYBER+INFRASTRUCTURE



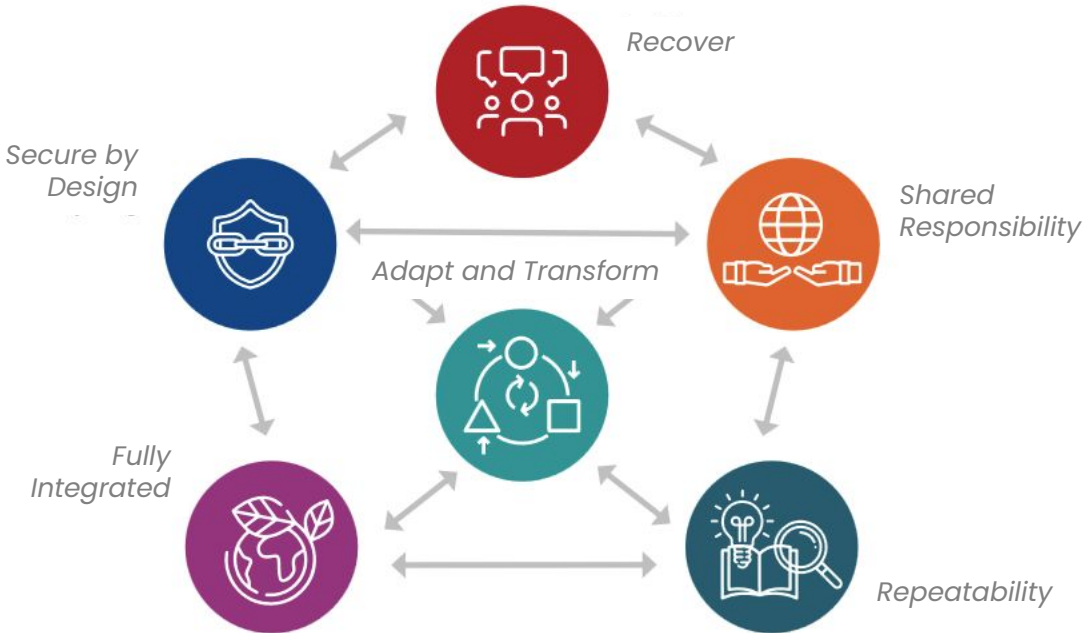
PCI Security Standards Council®

“Our approach must shift from a futile quest for absolute invulnerability to a more realistic strategy of resiliency in which we control the impacts of failures.”

*Strategy for Cyber-Physical Resilience
(White House - Feb 2024)*



Path to Resiliency: Isolated Management Infrastructure



Isolated Management Infrastructure

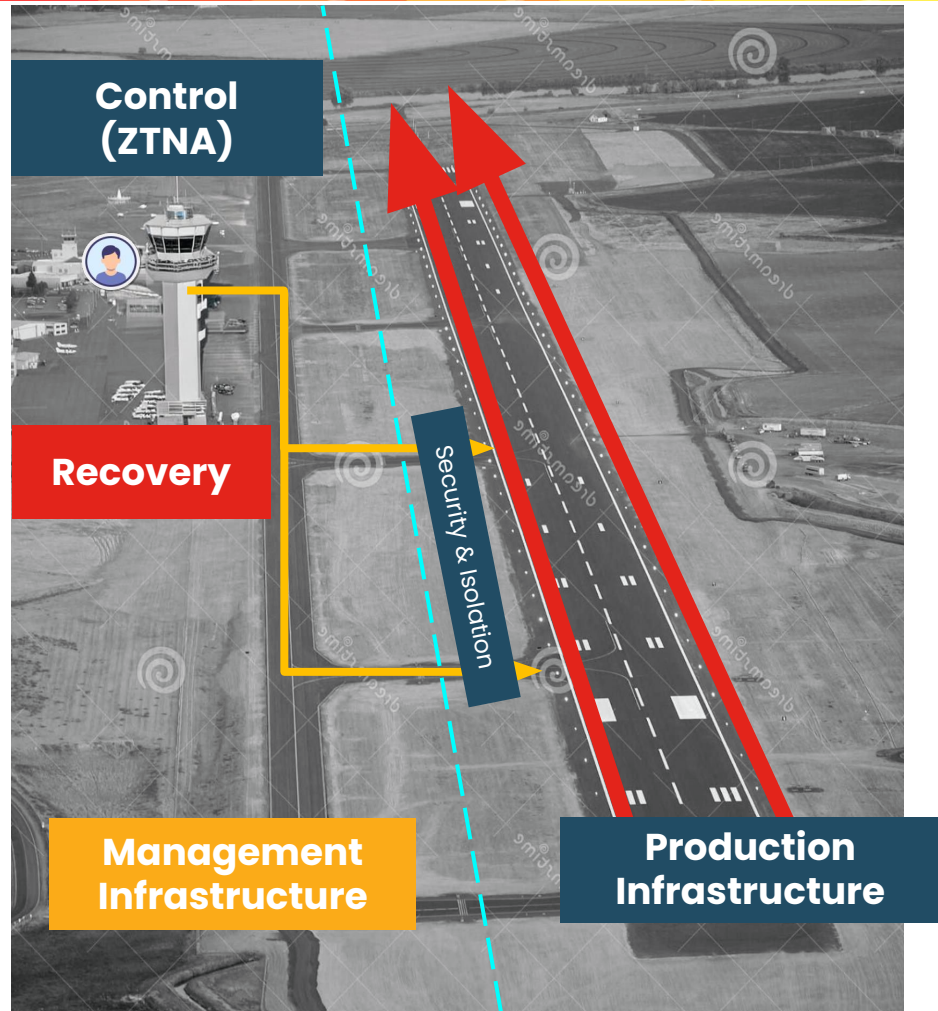
**Adapted from UNDRR Resilient Infrastructure Principles*

What is Isolated Management Infrastructure (IMI)?

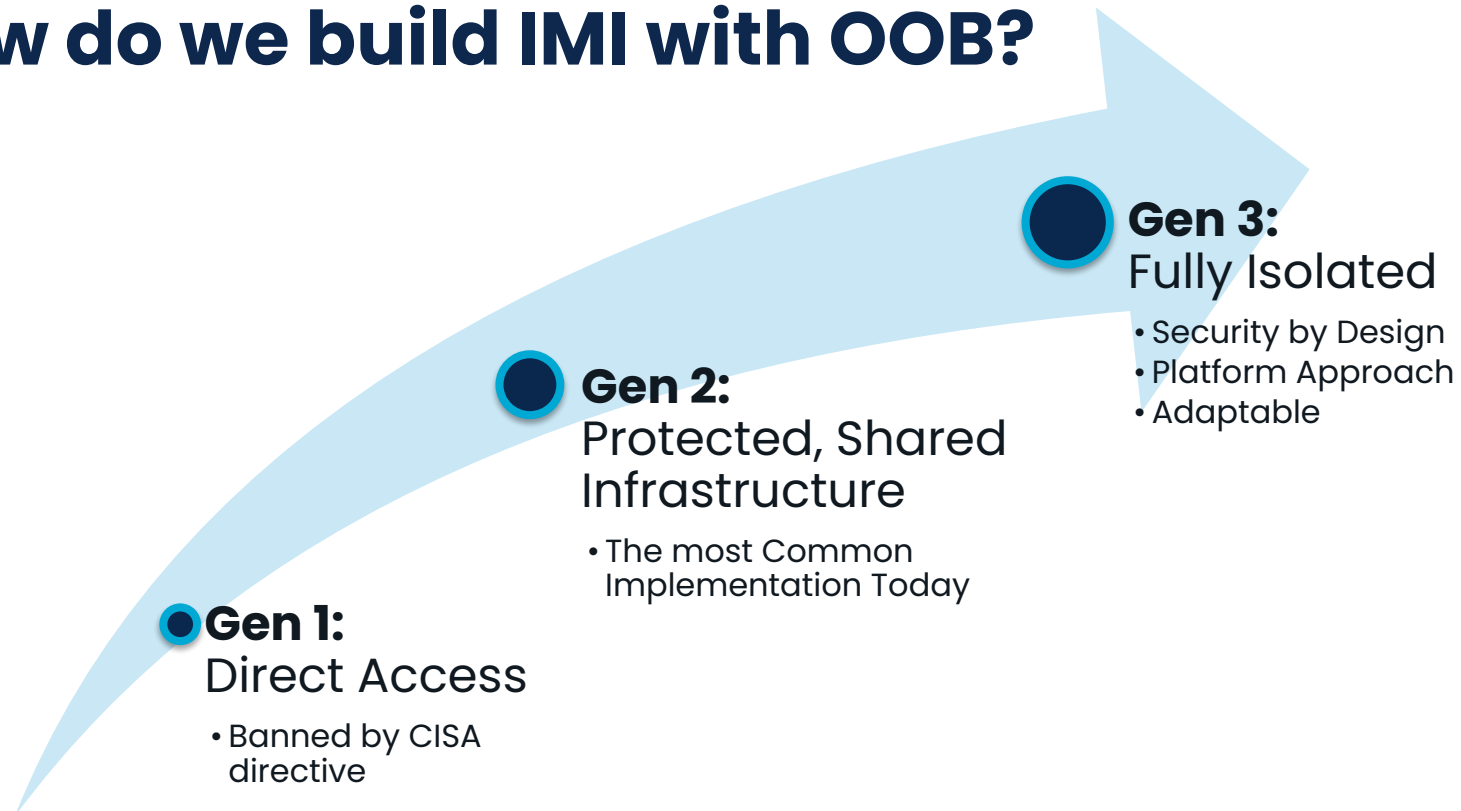
Think of **IMI** as an access road.

It is your direct line of access to the **Production Infrastructure** should you need it.

- Physical Segmentation (OOB) of Access to Management Infrastructure
- Control and Security (Zero Trust Principles)
- Recovery Tools
Backup and Restore
- Repeatability - Automation



How do we build IMI with OOB?



Gen 1:
Direct Access

- Banned by CISA directive

Gen 2:
Protected, Shared Infrastructure

- The most Common Implementation Today

Gen 3:
Fully Isolated

- Security by Design
- Platform Approach
- Adaptable

Gen 1: Direct Networked Management Interfaces

Banned by BOD 23-02 (CISA)

Control Plane Infrastructure

Remote Admin



What is it?

Gaps

Management Interfaces are directly accessible

No Separation

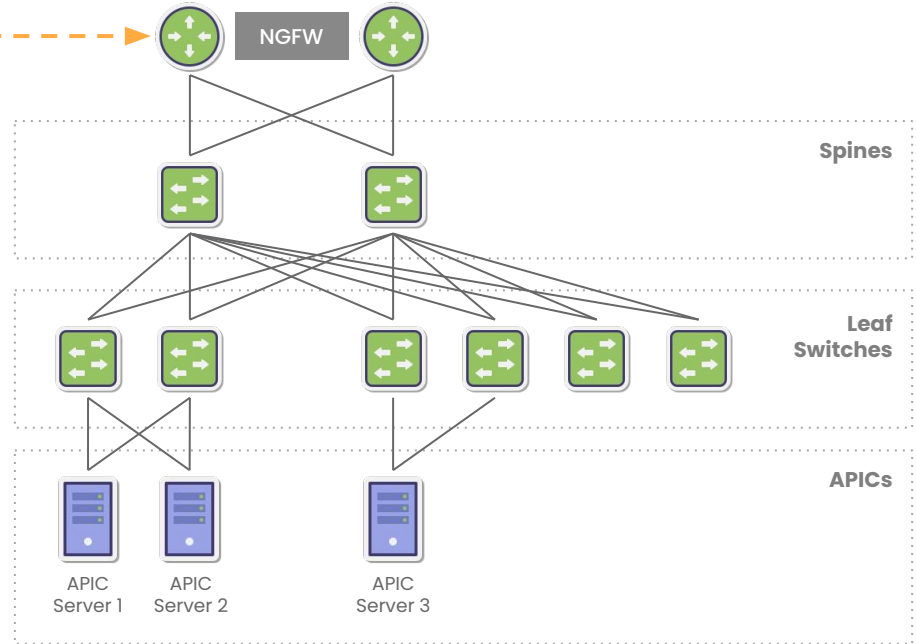
Admins use insecure protocols (RDP or Telnet)

Vulnerable Management Interfaces

No VPN is used to access management interfaces

Management Interfaces can be indexed and searched by the public

Production Infrastructure



Spines

Leaf Switches

APICs

APIC Server 1

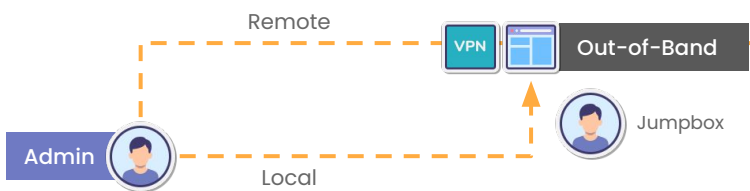
APIC Server 2

APIC Server 3

Gen 2: Protected Network Management Interfaces

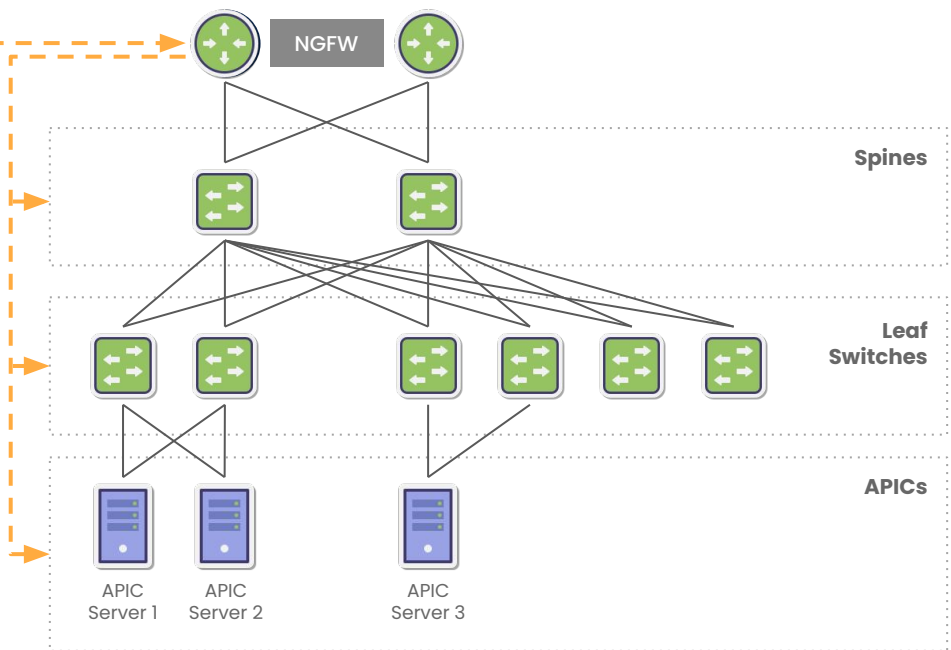
Acceptable by BOD 23-02 (CISA)

Control Plane Infrastructure



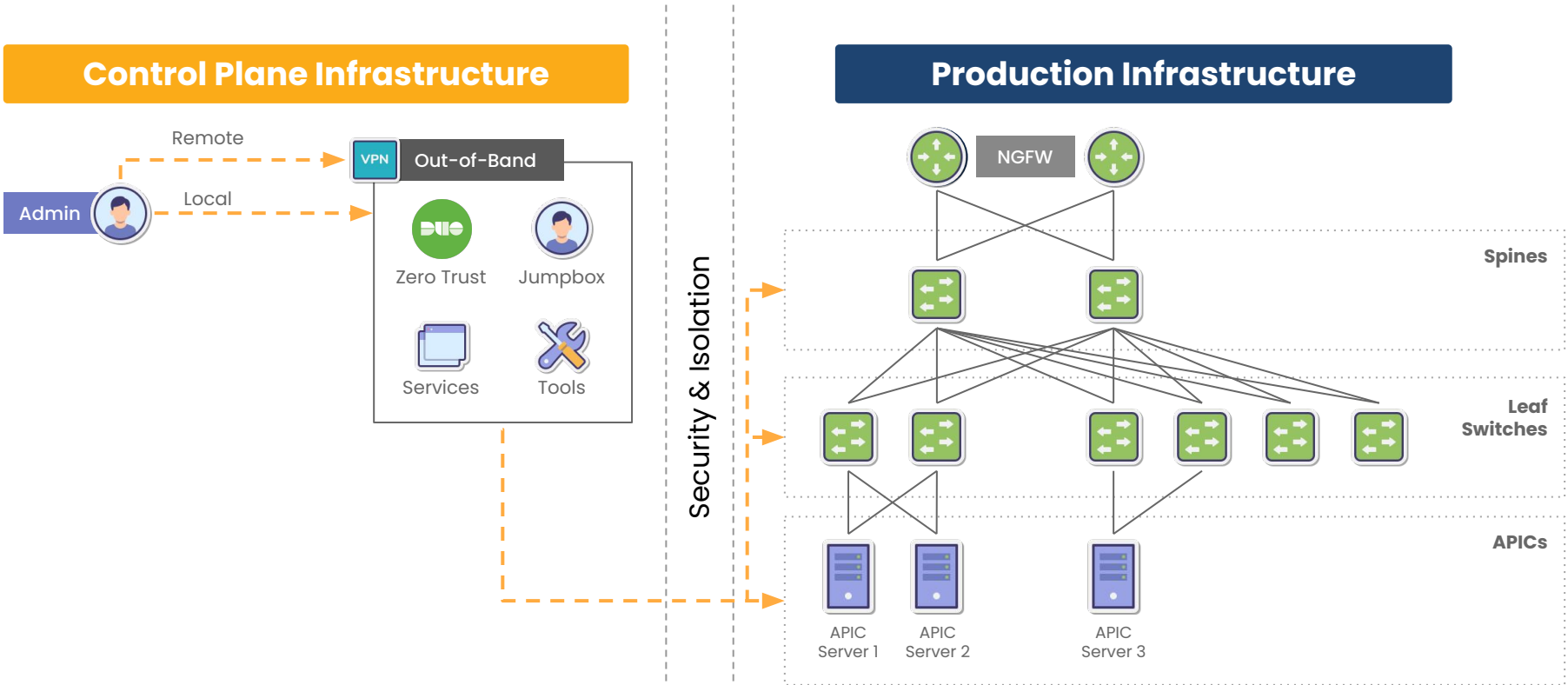
What is it?	Gaps
Management interfaces accessible via VPN only	No Separation
Admins use a mix of protocols	Vulnerable Management Interfaces
	Easy to jump between zones

Production Infrastructure



Gen 3: Isolated Management Infrastructure

Strongly Encouraged by BOD 23-02 (CISA)



What goes into implementing Isolated Management Infrastructure?



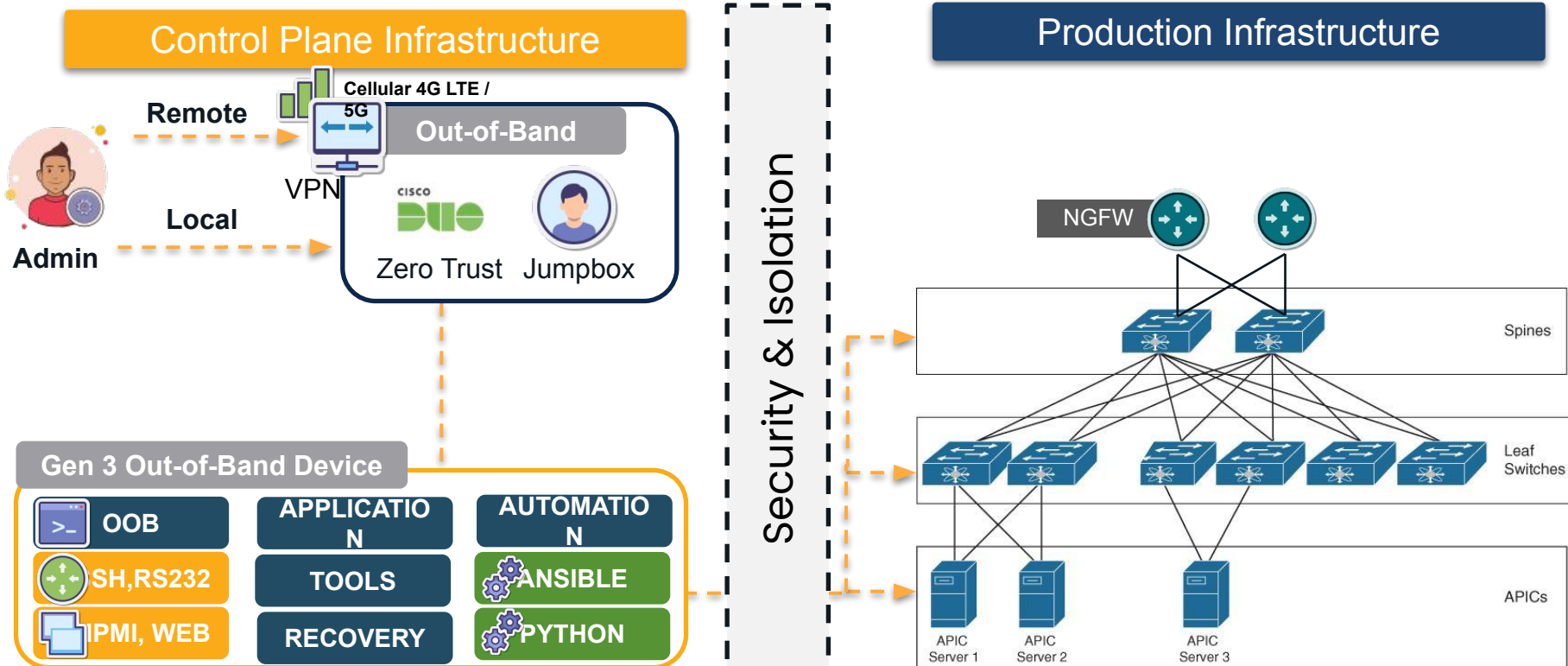
Applications

Infrastructure Automation	Ansible / Salt	ZTP	Python	DNA Center	ACI
Security	Hardware	VPN/Overlay	Patches	ZTNA	NGFW
Networking Services	Routing	Monitoring	DNS/DHCP /NTP	DNS/DHCP /NTP	Storage
Management Standards	RS232	Redfish	HTTPS	RESTful API	RDP/VPN API
Connectivity	OOB	LAN	WAN	4G/5G	Satellite
Hardware	Connectivity	Compute	Storage	Full Physical Isolation	Switching

Isolated Management Platform



Generation 3 Out-of-Band (OOB) Management design and deploy



cisco Live!

Benefits of Isolated Management Infrastructure based on Gen 3 OOB



Summary





The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive

CISCO *Live!*



GO BEYOND

#CiscoLive