TRUSTED BY 6 OF THE TOP 10 MOST VALUABLE GLOBAL TECH GIANTS

ZPE Systems Introduces Security Platforms for Enterprise

An Exclusive Presentation for **Security Field Day 7**

Koroush Saraf
VP, Product Management

Rene Neumann
Director of Solution Engineering

zpe® @ZPESystems info@ZPESystems.com

Agenda

Introduction: Why Cybersecurity for Enterprise Can't Be Solved By One Vendor

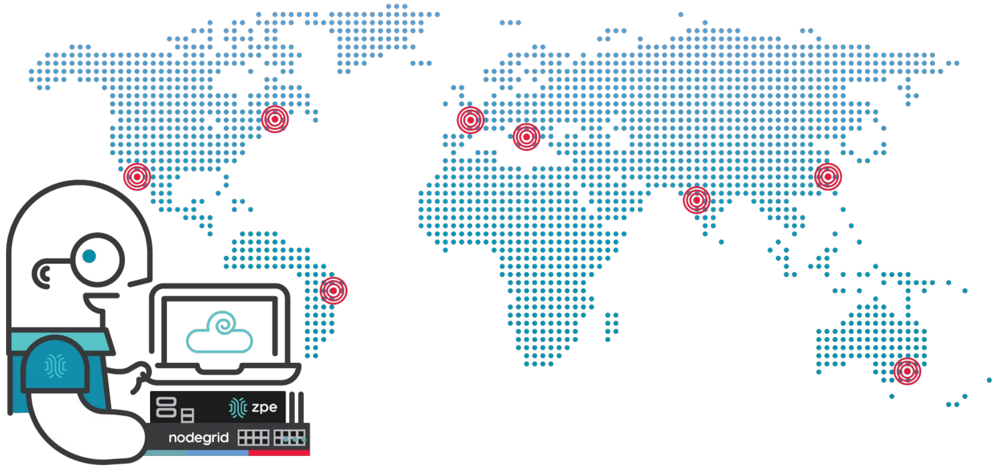
Cybersecurity vendors are at the top of their game. So why are cyber attacks increasing and becoming more effective? We'll discuss the modern enterprise's pain of having too many products, from too many different vendors, which leaves too many security gaps. We'll also discuss why this dynamic attack surface can't be solved simply by adding more products, and instead requires a platform — an automated and open platform capable of unifying the diverse ecosystem of cybersecurity solutions and eliminating gaps.

Demo No. 1: Immutable Principles of Branch Deployment

In this demo, we will show you how to overcome supply chain security risks and address ransomware by putting immutable infrastructure principles into action. We will demonstrate how to use SaltStack automation on our out-of-band platform, which we'll use to build, destroy, and re-build an edge data center — with ease and at scale.

Demo No. 2: Zero Pain Ecosystem | Launching Security Apps from ZPE's Cybersecurity Platform

In this demo, we will show our enterprise cybersecurity platform that powers what we call the Zero Pain Ecosystem. We will demonstrate the ease of use in securing remote branch locations, by using Horizon3's NodeZero to launch an automated pen test, and by running a Splunk agent to feed XDR systems. We will conclude this demo by showing how to use immutable principles for disaster recovery, to decommission an infrastructure stack and rebuild it automatically from scratch.



Hello!

We are ZPE Systems.

Founded: 2013
Headquarters: Silicon Valley, CA
Global & Enterprise Customers: >100

- ZPE Systems is an IT company that solves the networking problems of large enterprises – including 6 of the top 10 global tech giants – to help meet increasing demands for availability, security, and scalability

- Companies that maintain or operate many data centers and branch locations, such as those in healthcare, supply chain, government, and finance, trust ZPE's Intel-based serial consoles, services routers, and cloud management software to eliminate human error, security gaps, and interoperability issues

Customers

TRUSTED BY 6 OF THE TOP 10 GLOBAL TECH GIANTS

amazon

FINANCIAL SERVICES

VISA

BANK OF AMERICA

SEATTLE CREDIT UNION

SIG SUSQUEHANNA

SOCIETE GENERALE

MINTLY

RETAIL / ECOMMERCE

Mercedes-Benz

wish

LEROY MERLIN

ebay

GOVERNMENT

Australian Bureau of Statistics

Ontario

HM Revenue & Customs

HEALTHCARE

HCA Healthcare®

Helsana

COMMUNICATIONS

Vapor

gtt

HEAnet
Ireland's National Education & Research Network

Post Luxembourg

ip max

ENERGY

NFON
Cloud Telephone System

Schlumberger

MEDIA

Time Warner Cable®

Mediacom

COMCAST

EDUCATION

M

VT VIRGINIA TECH

USC University of Southern California
Information Sciences Institute

TECHNOLOGY / INDUSTRIAL

Uber

digicert®

DELTA

STACKPATH™

Koç

Introduction

Why Cybersecurity for Enterprise Can’t Be Solved by One Vendor

Koroush Saraf
VP, Product Management

Problems in Cybersecurity

Ransomware & Supply Chain

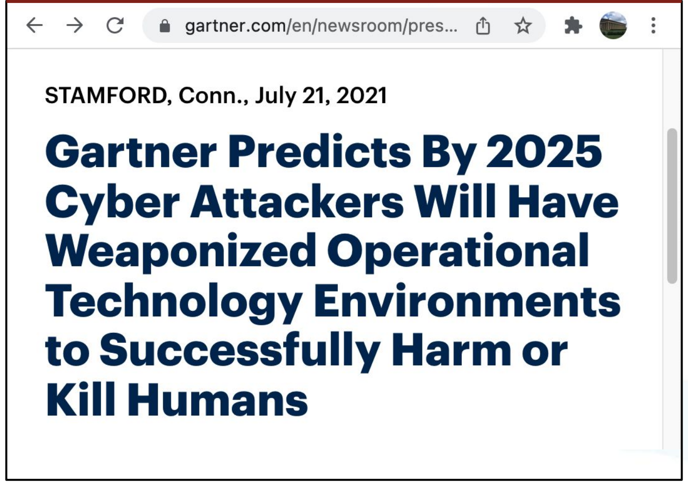
Kaseya (2021)

JBS (2021)

Colonial Pipeline (2021)

CNA Financial (2021)

Attacks on Operational Infrastructure (OT)



STAMFORD, Conn., July 21, 2021

Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans

Holistic Security

Hard to operate

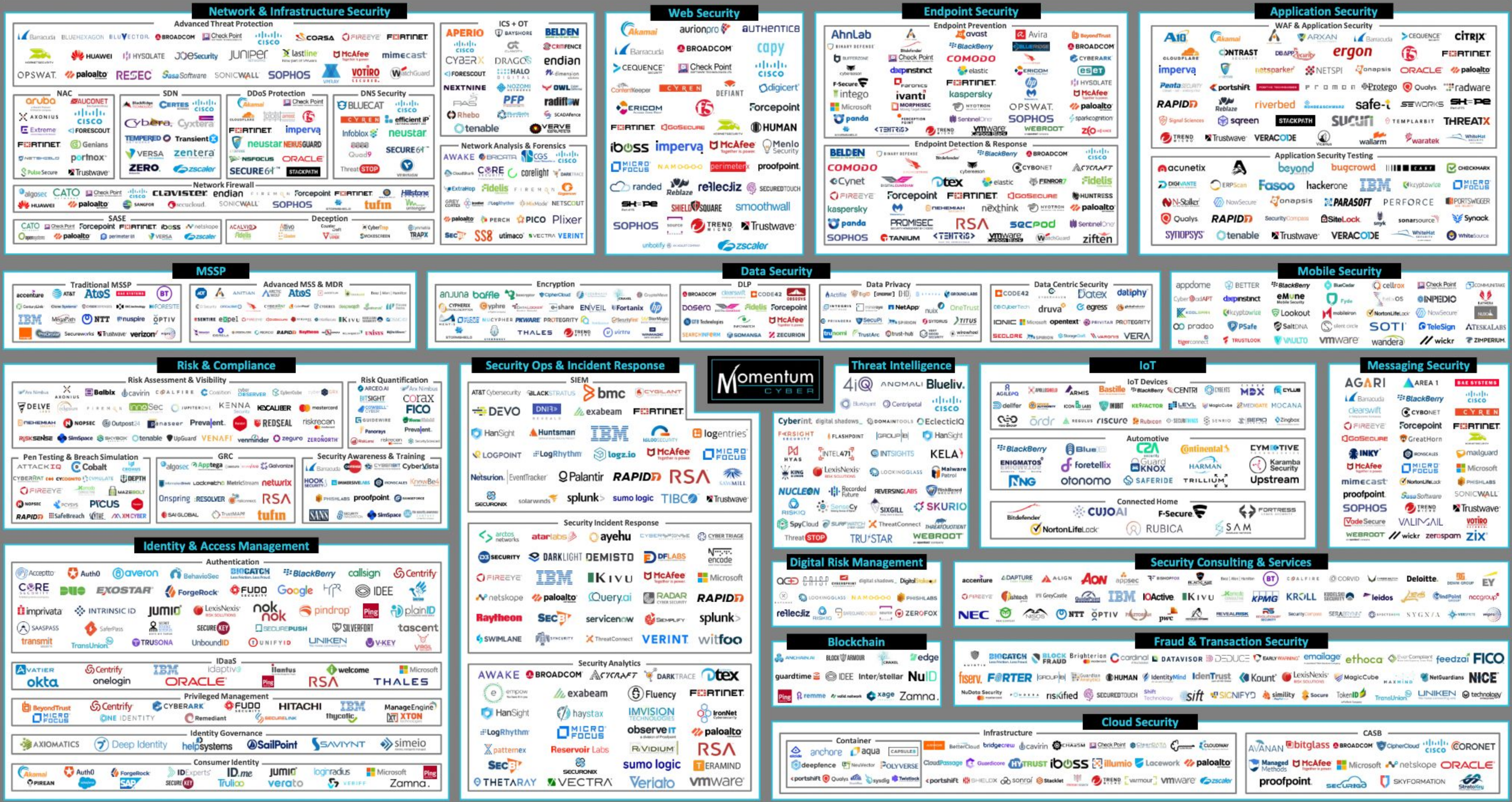
Have to trust my partners

Hybrid Infrastructure

CYBERSCAPE

Too many products. Too many experts. Too many gaps.

2021



Examples from Customers

- Palo Alto + 128T SD-WAN at 1,000 branches
- Convergence of IT and OT - Needs special segmentation engine
- Pen test needs a launching pad at branch locations

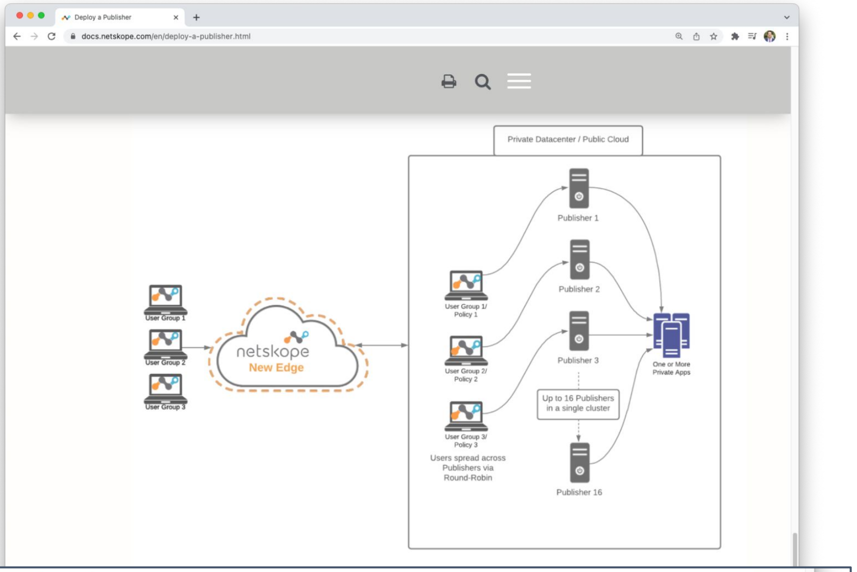
- Migration from public cloud back to private cloud or Hybrid
- Secure by Design, Network as Code → How do you do it?
- How do I implement all the products for: IEC 62443, MITRE, NIST

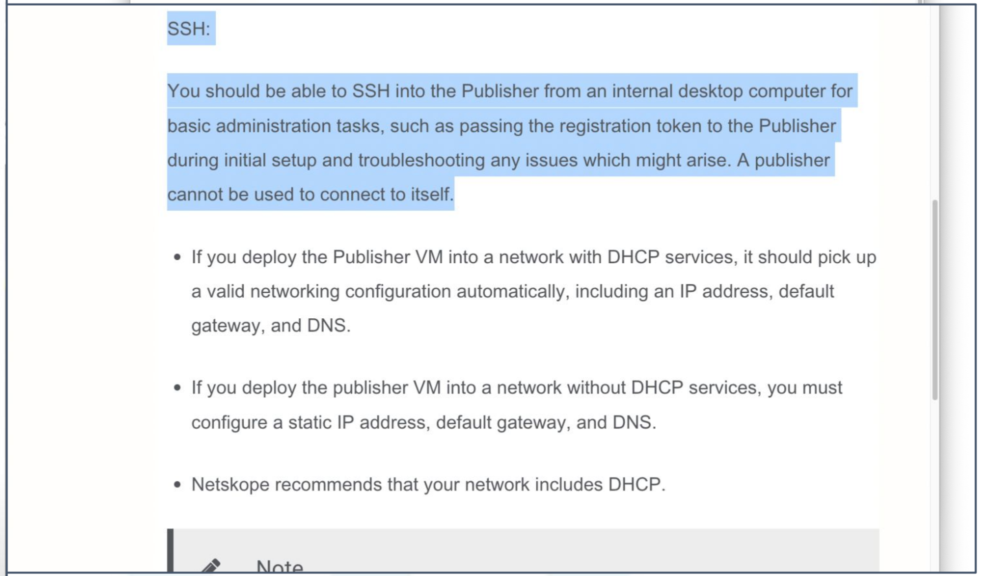
The pain in cybersecurity is from difficulty of deployment and unpredictable operation of multi-vendor ecosystem parts

ZTNA – Zero Trust Network Access Implementation

Where does IT install the ZTNA publisher at edge locations?

Where do I install the ZTNA client at my branch office?



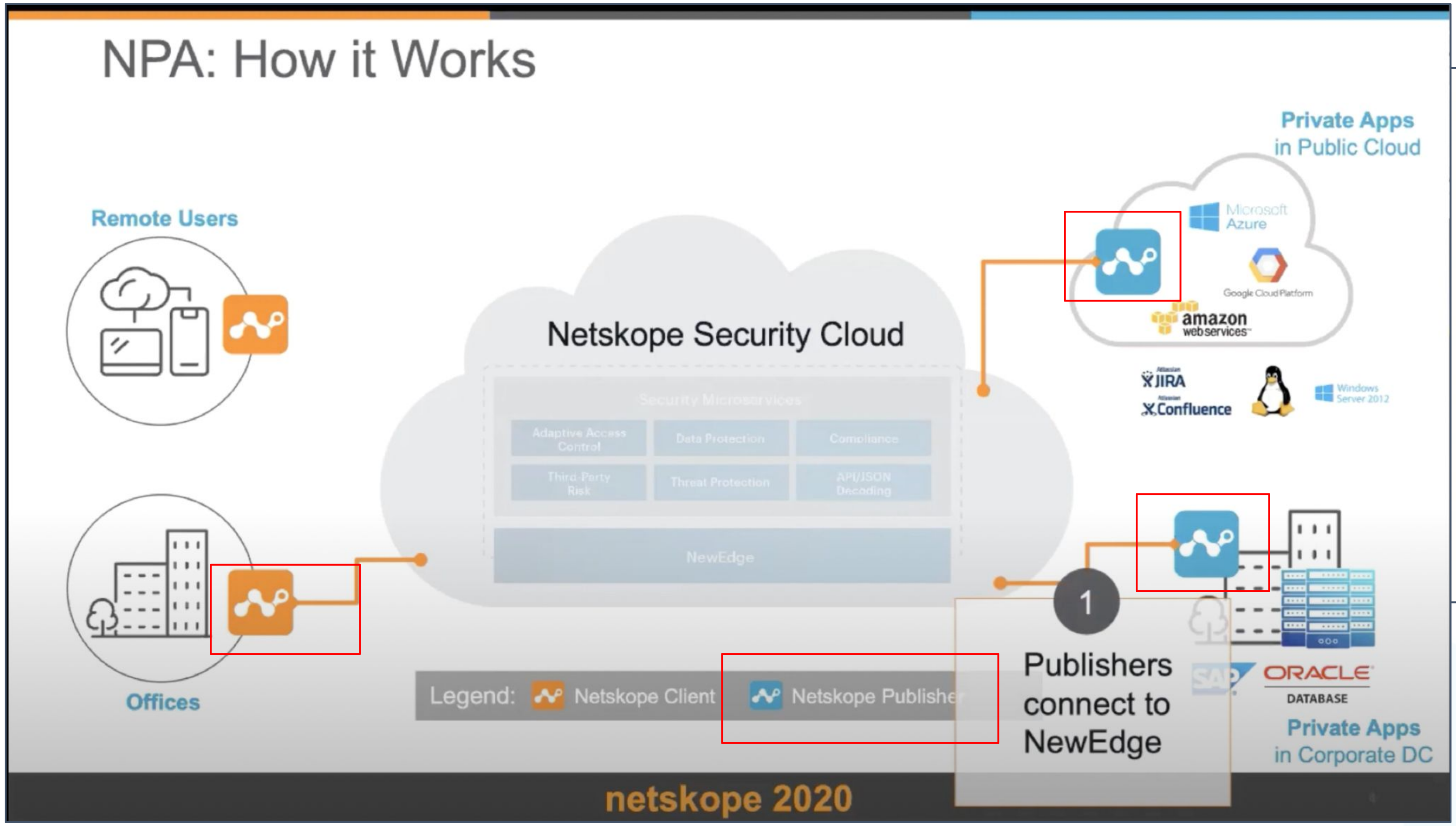


SSH:

You should be able to SSH into the Publisher from an internal desktop computer for basic administration tasks, such as passing the registration token to the Publisher during initial setup and troubleshooting any issues which might arise. A publisher cannot be used to connect to itself.

- If you deploy the Publisher VM into a network with DHCP services, it should pick up a valid networking configuration automatically, including an IP address, default gateway, and DNS.
- If you deploy the publisher VM into a network without DHCP services, you must configure a static IP address, default gateway, and DNS.
- Netskope recommends that your network includes DHCP.

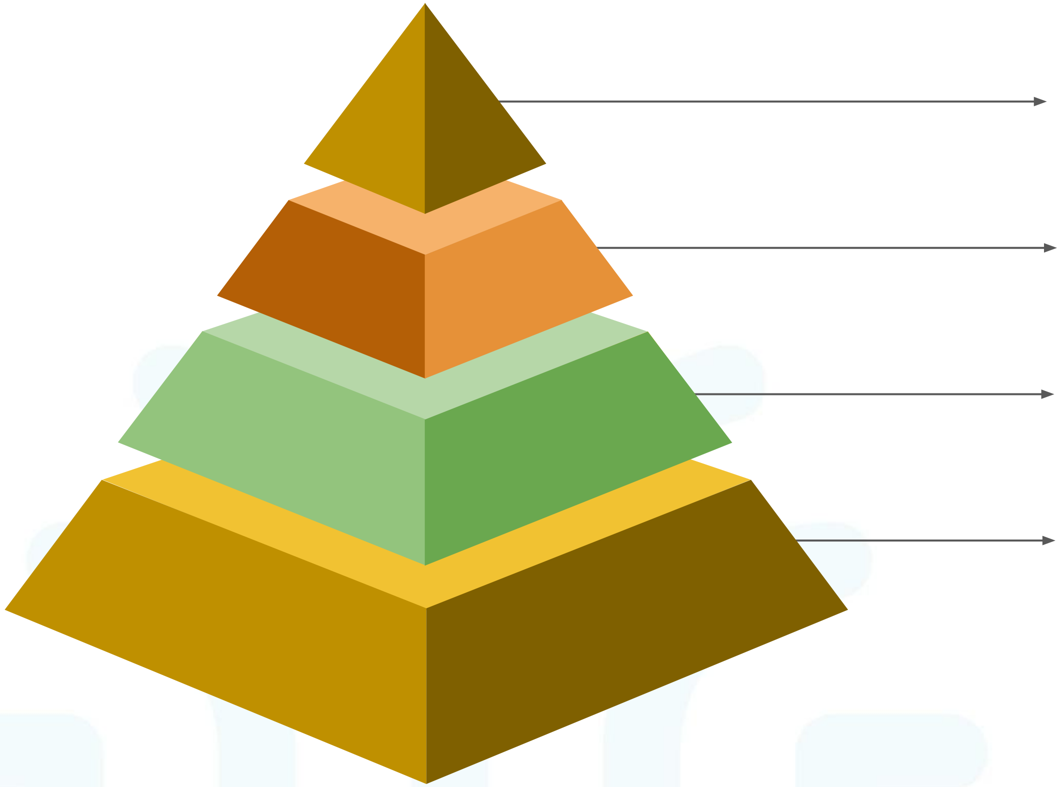
Note



NPA: How it Works

1 Publishers connect to NewEdge

Cybersecurity Ecosystem at Enterprise



Management & Automation: AiOps, SecOps, NetOps, DevXxxOps

Security Apps: NGFW, Pen Test, XDR Probe, ZTNA Publisher

SW Platform

HW Platform

Cybersecurity Ecosystem at Enterprise

Source: https://commons.wikimedia.org/wiki/File:In-n-out_3x3_Burger.jpg

Management / Visualization

- AIOPS
- Orchestration / Automation
- Management
- Monitoring

Security Apps

- NGFW,
- XDR Probe, Pen Test
- ZTNA Publisher
- SASE On-Ramp

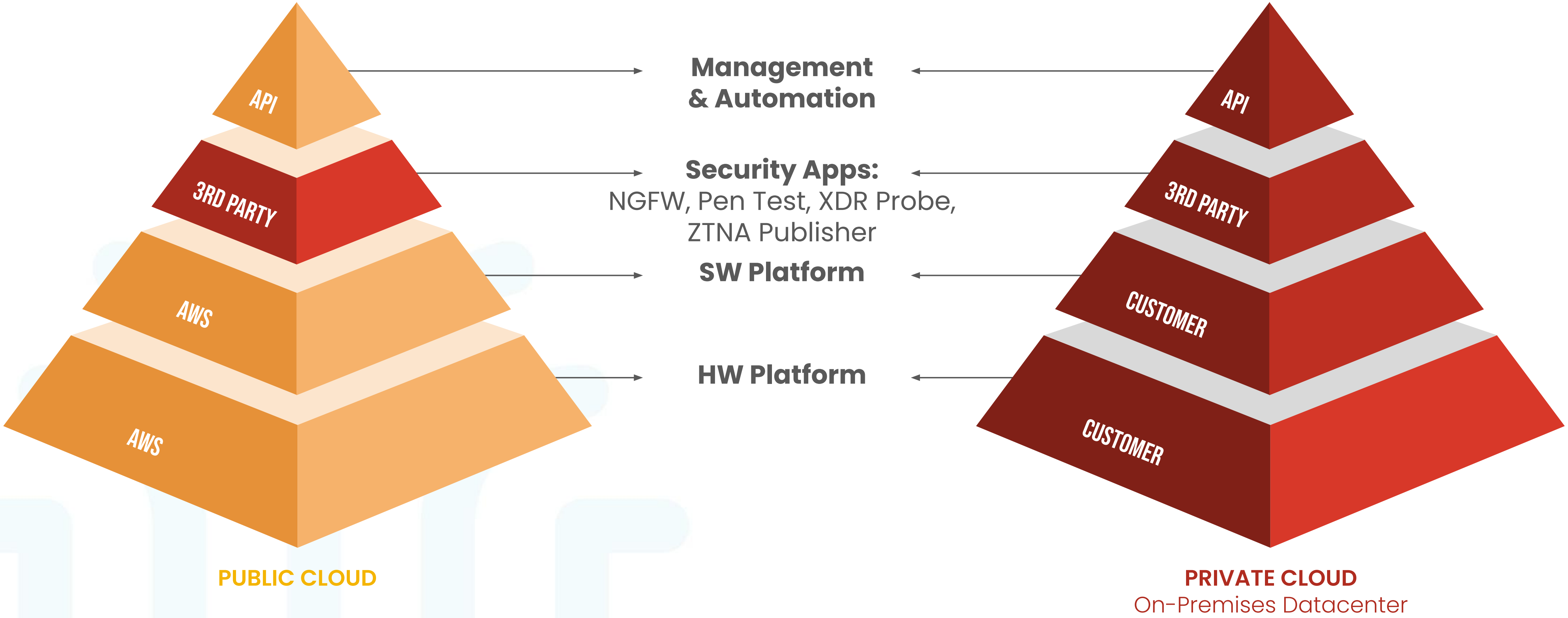
SW

- Secure OS
- Docker / Hypervisor
- Out-of-Band
- Zero Touch Provisioning

HW

- Single Platform
- Rich Interfaces
- TPM, Encrypted Disk, Zero Trust Boot

Cybersecurity Ecosystem at Hybrid Enterprise



Management & Automation

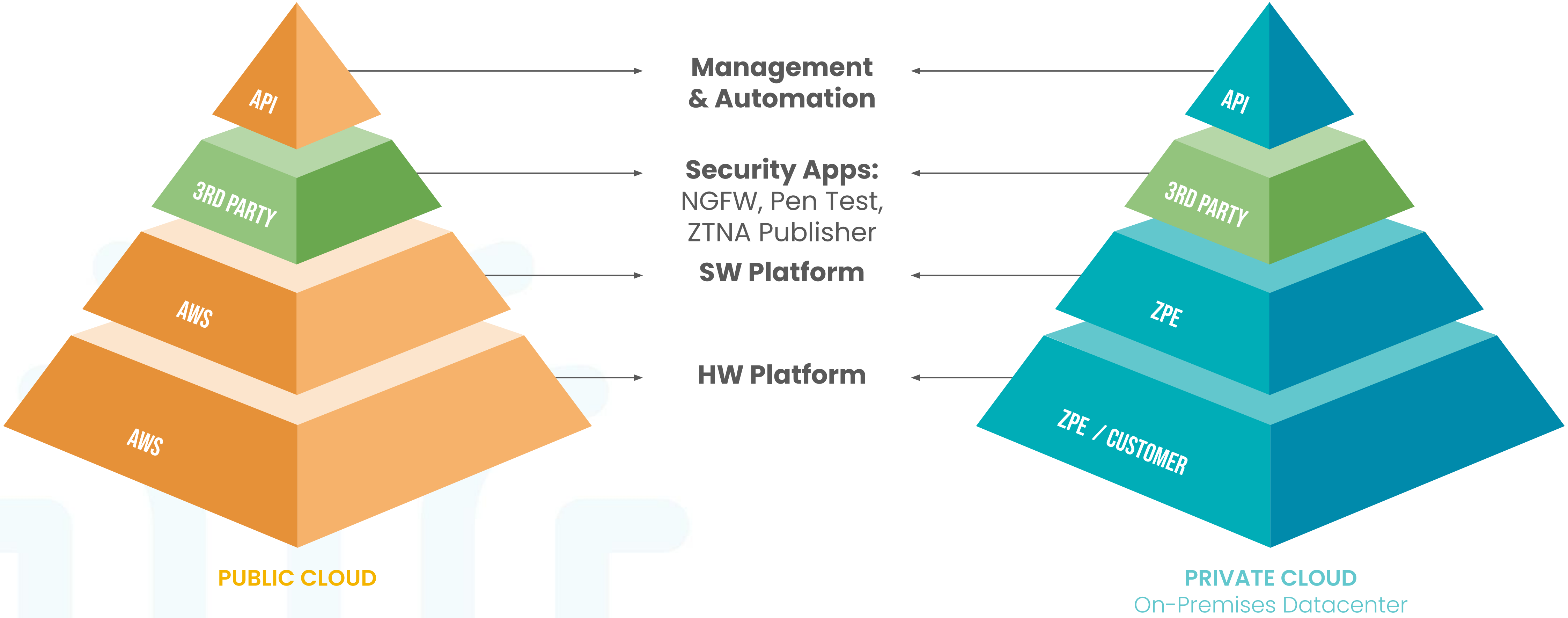
Security Apps: NGFW, Pen Test, XDR Probe, ZTNA Publisher

SW Platform

HW Platform

info@ZPEsystems.com @ZPEsystems zpe

Cybersecurity Ecosystem at Hybrid Enterprise with ZPE

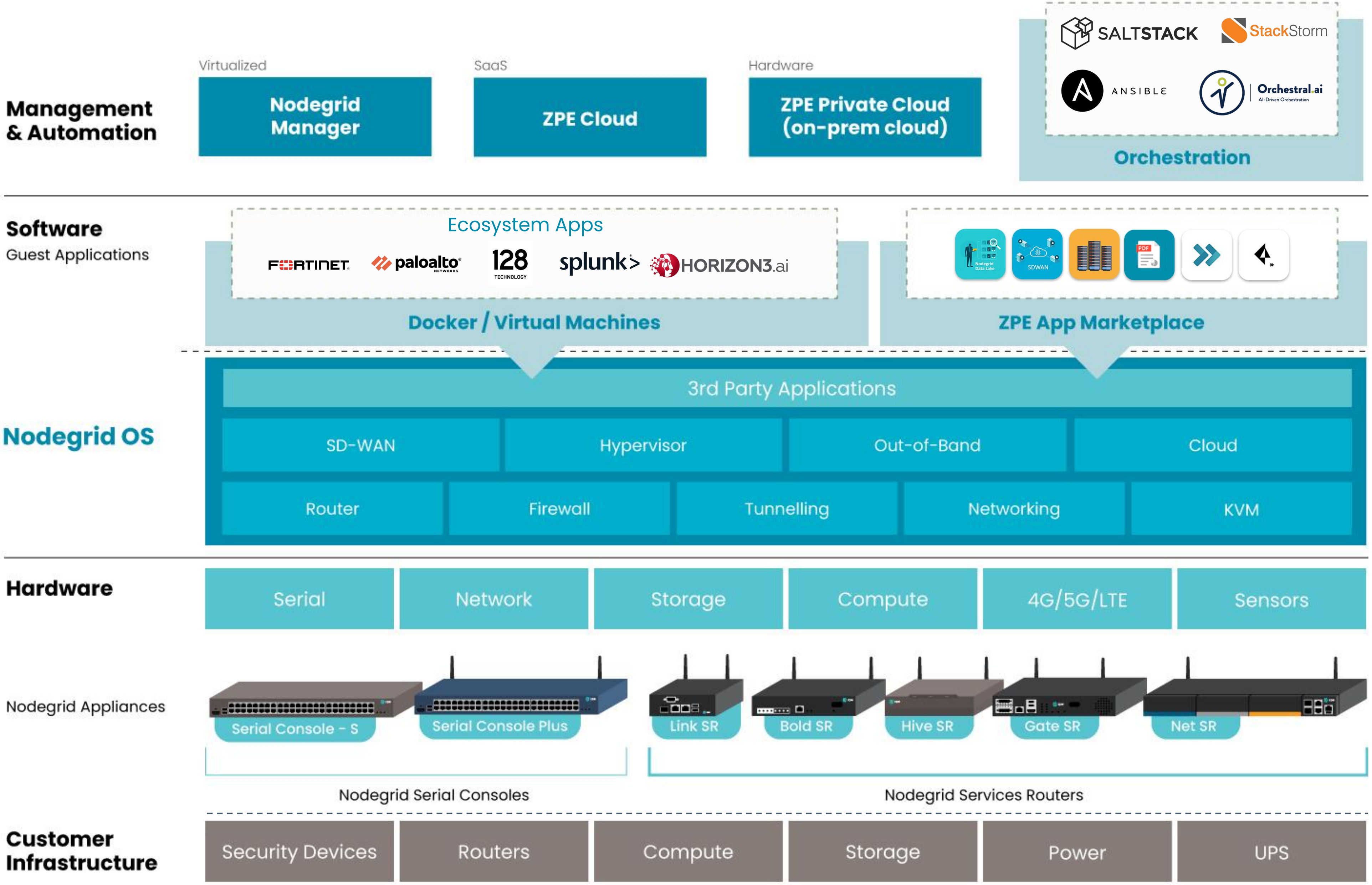


Management & Automation

Security Apps:
NGFW, Pen Test,
ZTNA Publisher

SW Platform

HW Platform



Management & Automation

- Virtualized: Nodegrid Manager
- SaaS: ZPE Cloud
- Hardware: ZPE Private Cloud (on-prem cloud)

Orchestration: SALTSTACK, StackStorm, ANSIBLE, Orchestral.ai (AI-Driven Orchestration)

Software
Guest Applications

Ecosystem Apps: FORTINET, paloalto NETWORKS, 128 TECHNOLOGY, splunk>, HORIZON3.ai

Docker / Virtual Machines

ZPE App Marketplace: Nodegrid Data Lake, SDWAN

Nodegrid OS

3rd Party Applications

SD-WAN | Hypervisor | Out-of-Band | Cloud

Router | Firewall | Tunnelling | Networking | KVM

Hardware

Serial | Network | Storage | Compute | 4G/5G/LTE | Sensors

Nodegrid Appliances

- Nodegrid Serial Consoles: Serial Console - S, Serial Console Plus
- Nodegrid Services Routers: Link SR, Bold SR, Hive SR, Gate SR, Net SR

Customer Infrastructure

Security Devices | Routers | Compute | Storage | Power | UPS

ZPE Private Cloud Platform with OOB Automation

Cybersecurity Platform at Edge

Router / SD-WAN

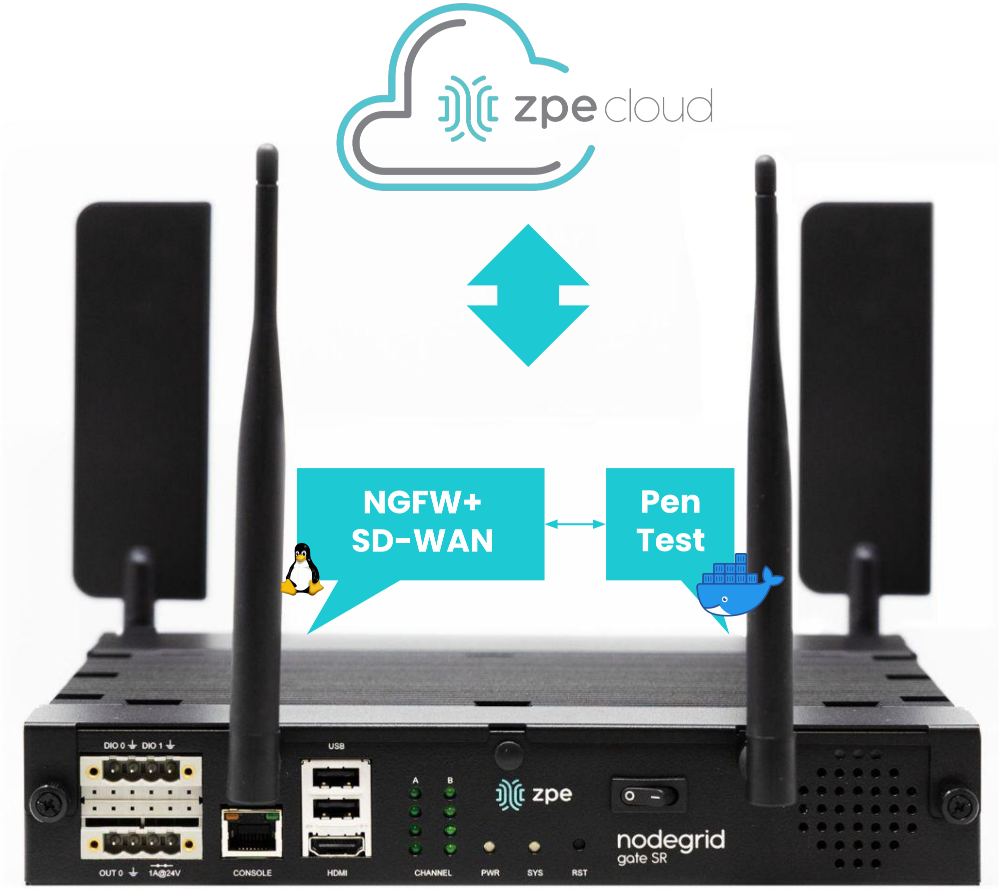
Cellular APs

Switch

Firewall

Out-of-Band
Console Switch

Automation &
Jumpbox Server



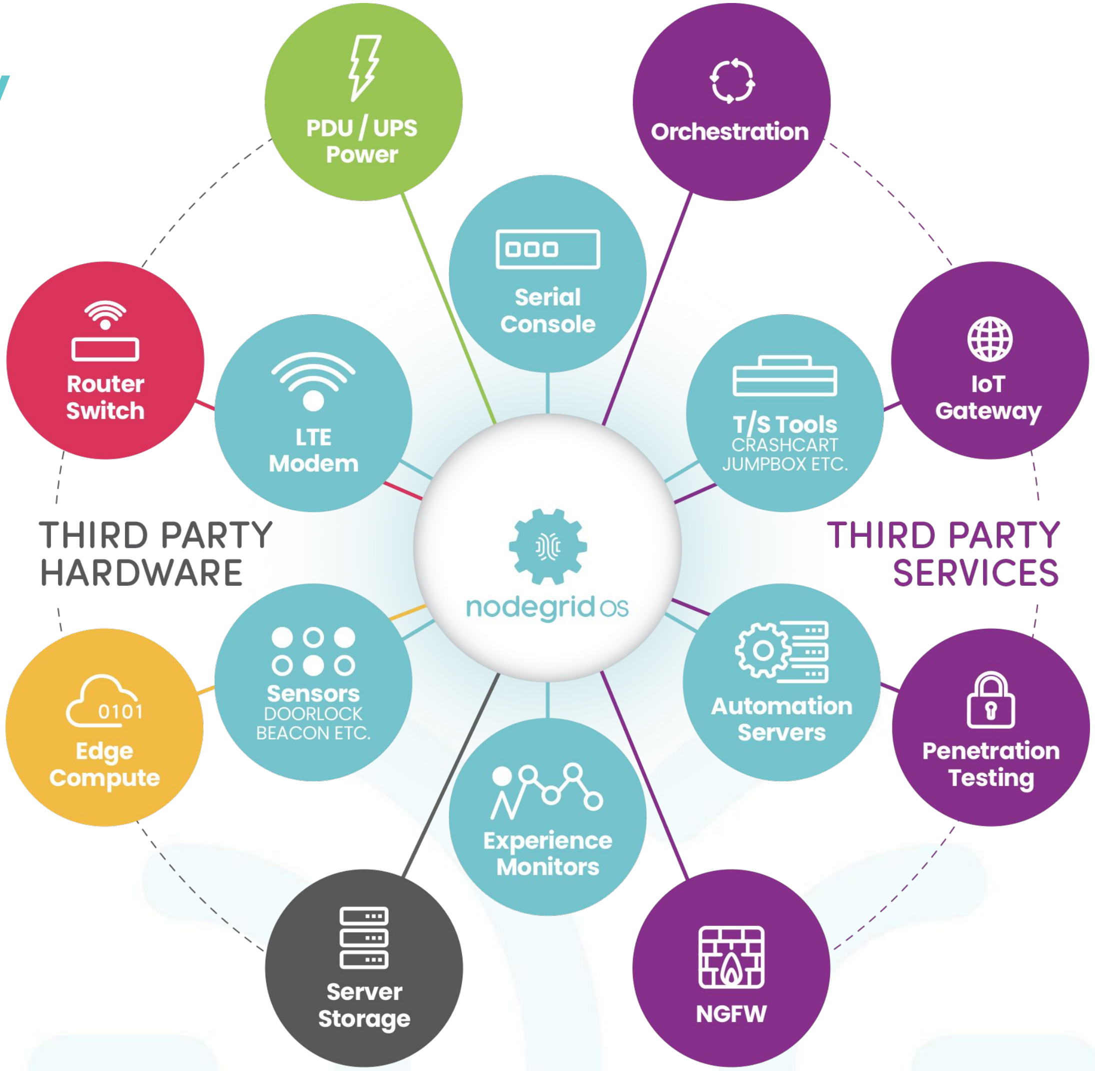
Nodegrid Gate SR (GSR-T8-BASE)

$$$$$ $$

Prolonged downtime, truck rolls, etc.

Near 100% uptime, agility, cost savings

Cybersecurity is a Team Sport



🟦 ZPE Systems Scope

Zero Pain Ecosystem

Immutable Principles of Branch Deployment

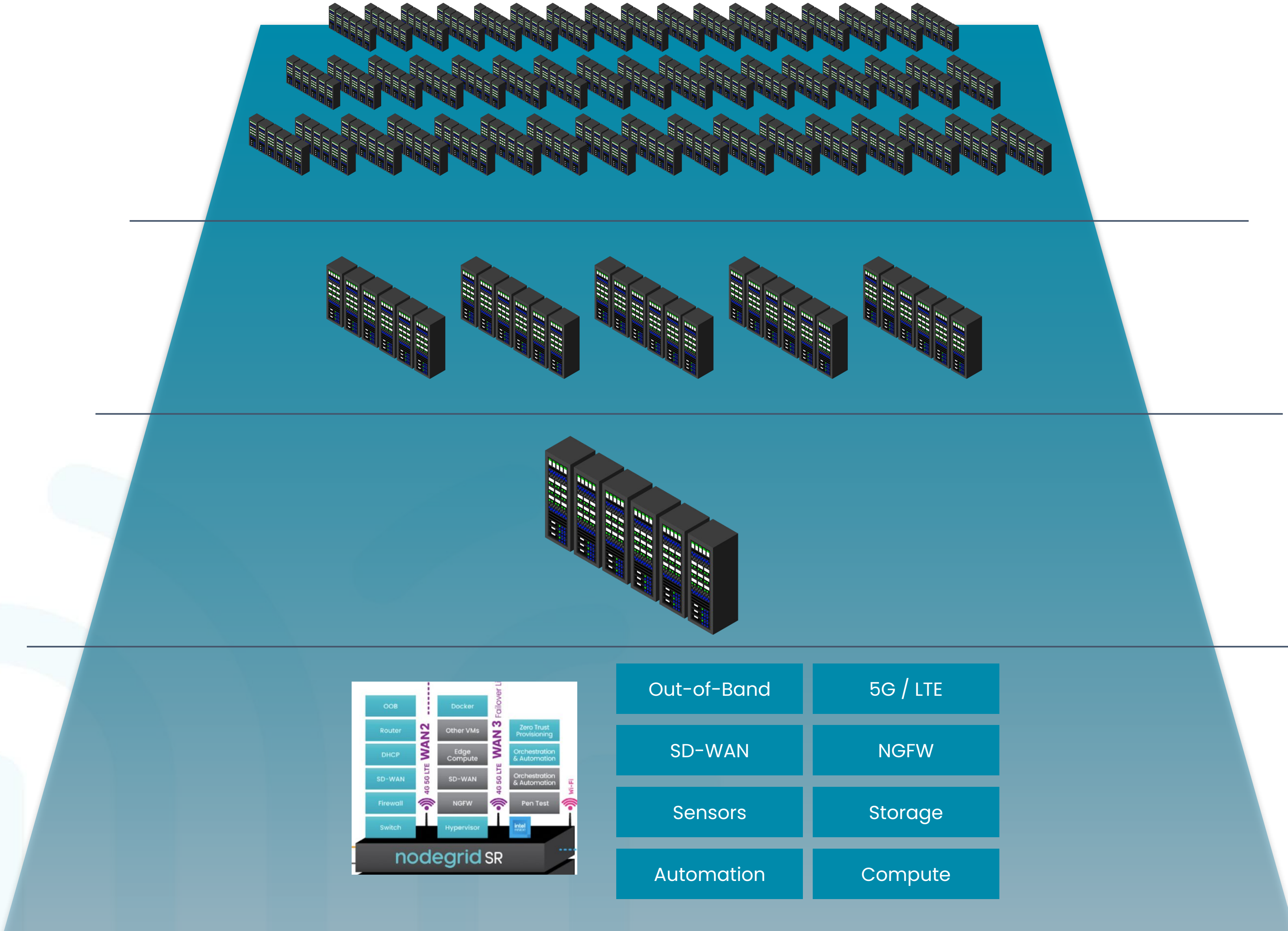
Demo No. 1

zpe® info@ZPEsystems.com @ZPEsystems

Rene Neumann
Director of Solution Engineering

Enabling Private Cloud from Hyperscale Datacenter to the Edge

info@ZPEsystems.com @ZPEsystems zpe



Out-of-Band
5G / LTE
SD-WAN
NGFW
Sensors
Storage
Automation
Compute

Hyperscale Datacenter
1000+ Racks

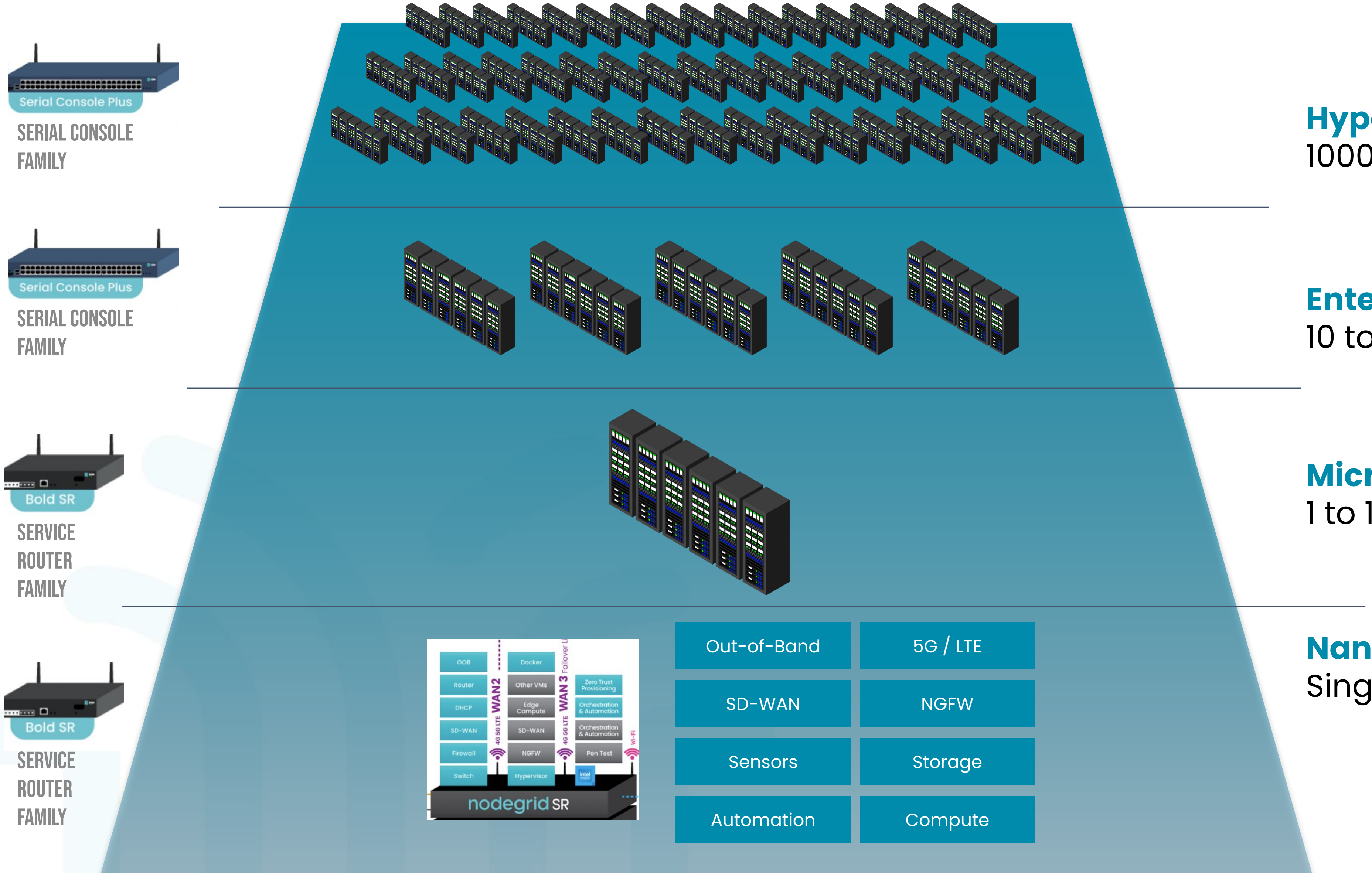
Enterprise Datacenter
10 to 1000 racks

Micro - Edge Datacenter / Colo
1 to 10 racks

Nano - On-premise Edge
Single Server

Enabling Private Cloud from Hyperscale Datacenter to the Edge

info@ZPEsystems.com @ZPEsystems zpe



SERIAL CONSOLE FAMILY

Hyperscale Datacenter
1000+ Racks

SERIAL CONSOLE FAMILY

Enterprise Datacenter
10 to 1000 racks

SERVICE ROUTER FAMILY

Micro - Edge Datacenter / Colo
1 to 10 racks

SERVICE ROUTER FAMILY

Nano - On-premise Edge
Single Server

Out-of-Band	5G / LTE
SD-WAN	NGFW
Sensors	Storage
Automation	Compute

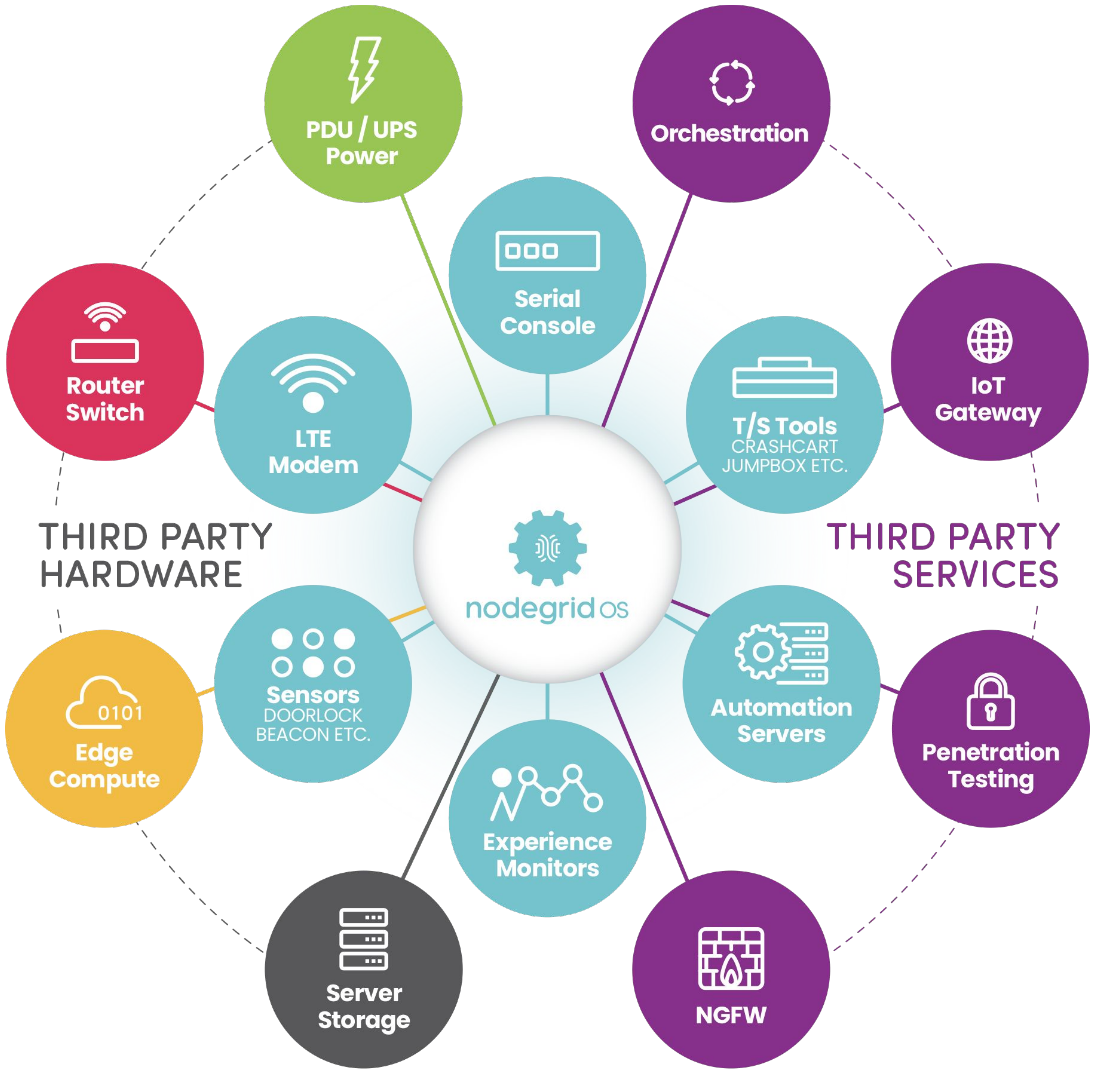
Goals for Infrastructure Operations

01	Secure	- Vendor and Transport - Physical Local Security - Solution Integrity
02	Simple	- Design must be simple to deploy - Process must support irritative changes and improvements - Can be maintained and supported for multiple years
03	Scalable	- Process needs to be repeatable to 100's or 1000's location - Support ongoing improvements - Is simple teachable to other groups or new team members
04	Sustainable	- Solution is expandable/flexible to support changes - Solution is future prove
05	Sensible	- Solution supports all current requirements - Solution supports future requirement changes - Costs are within business expectations

DEMO 1

Immutable Principles for Security

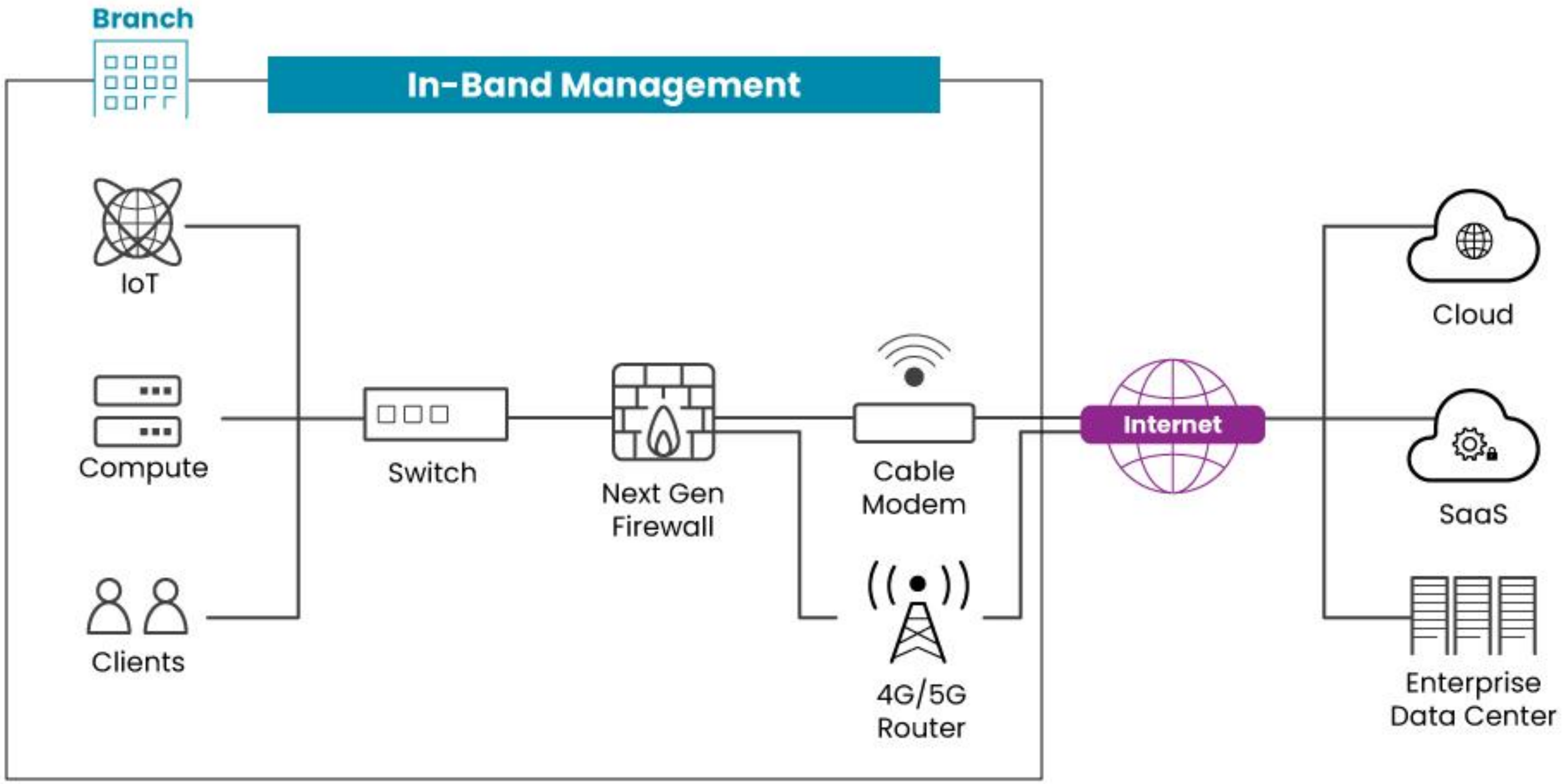
- Build, destroy, rebuild an edge infrastructure
- Demonstrating the same immutable principles learned from public cloud & tech giants
    - ○ Secure initial deployment
    - ○ Recover infected infrastructure
    - ○ Deploy changes holistically
    - ○ Ensure certainty of deployment outcome
    - ○ Roll back to the known good state



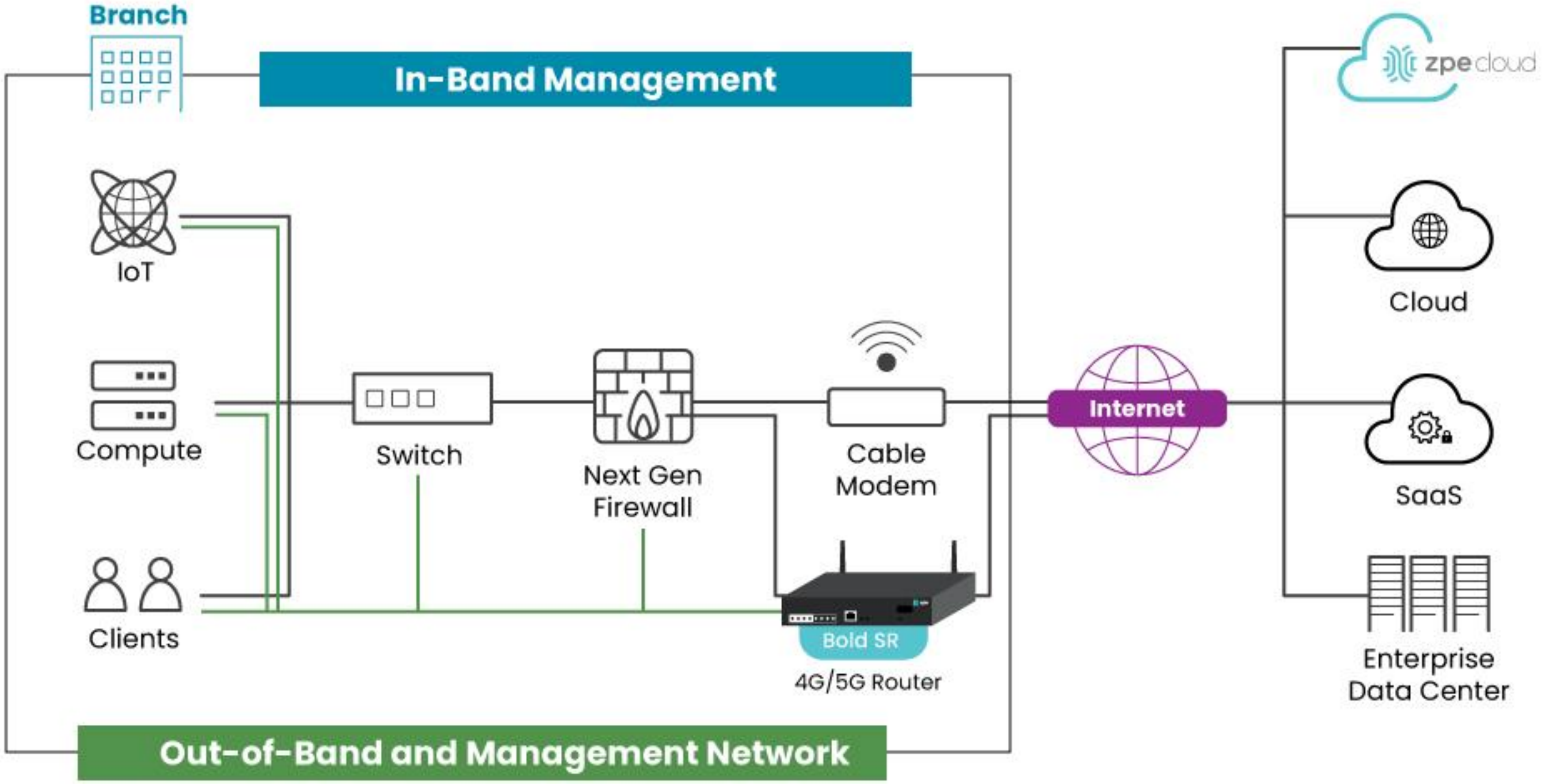
Zero Pain Ecosystem

🟦 ZPE Systems Scope

Common Edge Data Center Deployment



Edge Data Center Deployment with Nodegrid



REMOTE OFFICE | BRANCH SOLUTIONS

Nodegrid Bold SR

IT Infrastructure Management for the Branch: The ultimate fully loaded branch device for Guest OS, OOB, 4G/LTE Cellular Failover solution.

CPU
4 core
Intel x86
64-bit CPU

DRAM
4 to 8GB of
DDR3 DRAM

Storage
32GB to 2TB
Self-Encrypted Disk

Wi-Fi
2x2 Wi-Fi 5

5G / 4G / LTE
Shared OOB
& In-Band

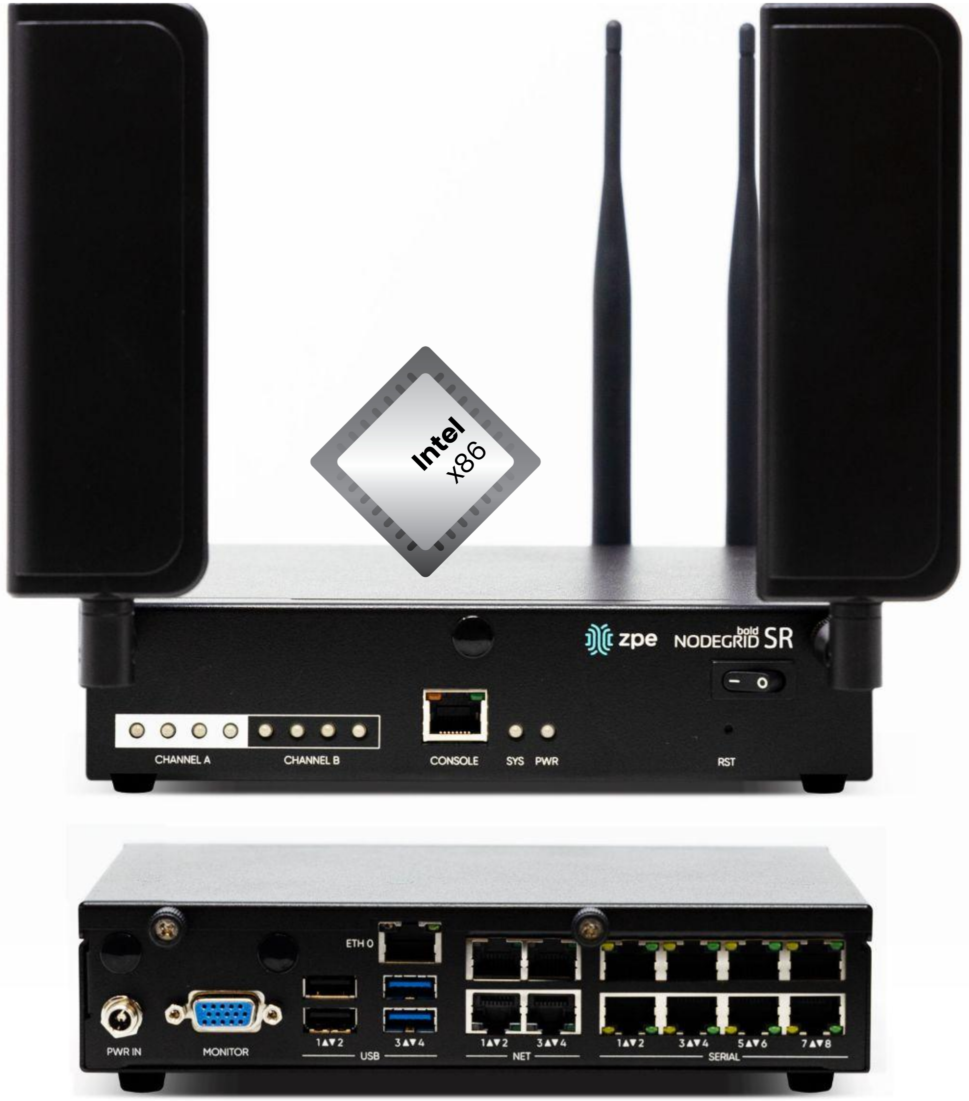
Edge Compute

OS
Nodegrid OS
Linux

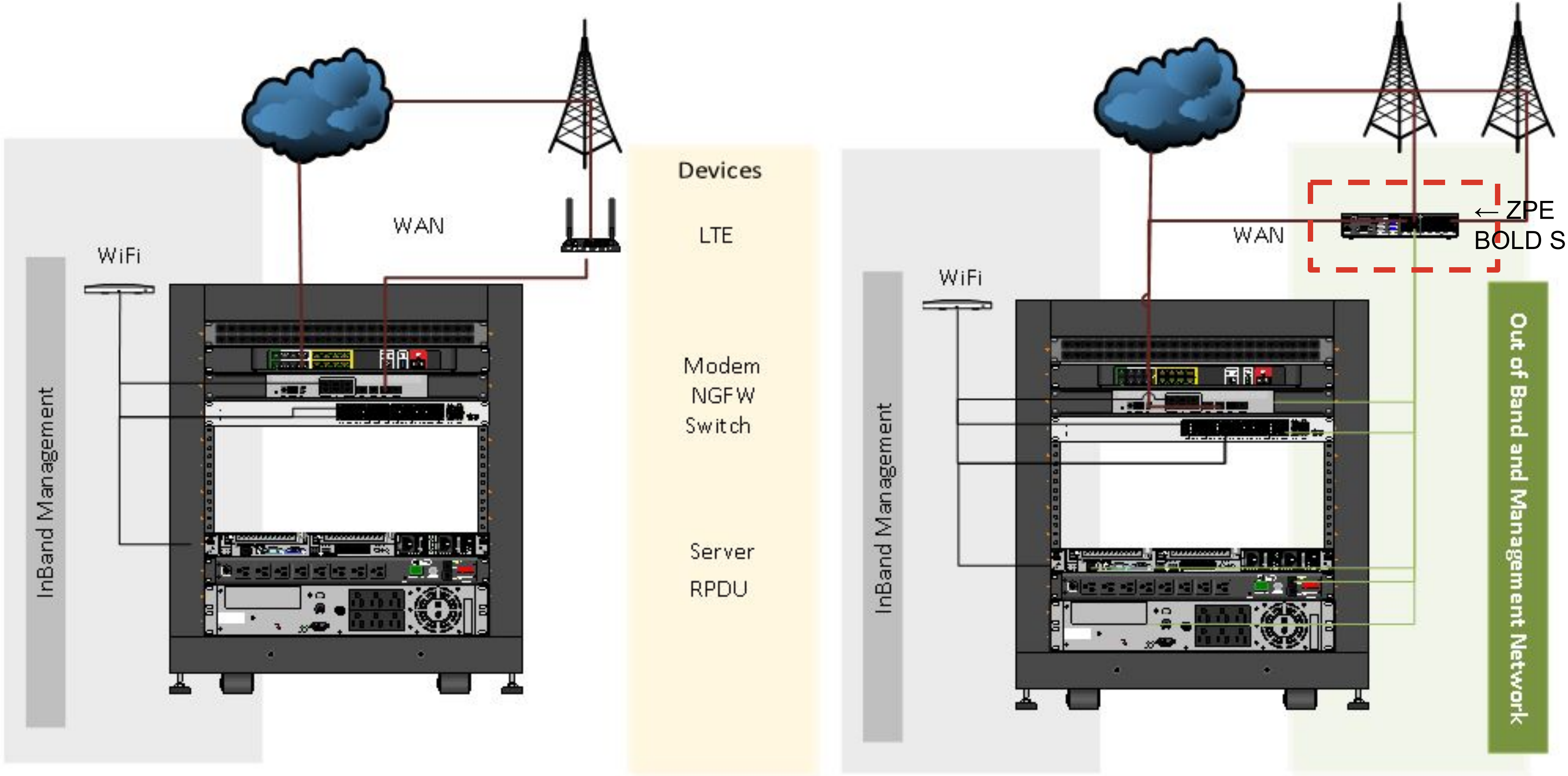
Serial
8X RJ-45
4X USB

Ethernet
5X Gigabit
with VLAN option

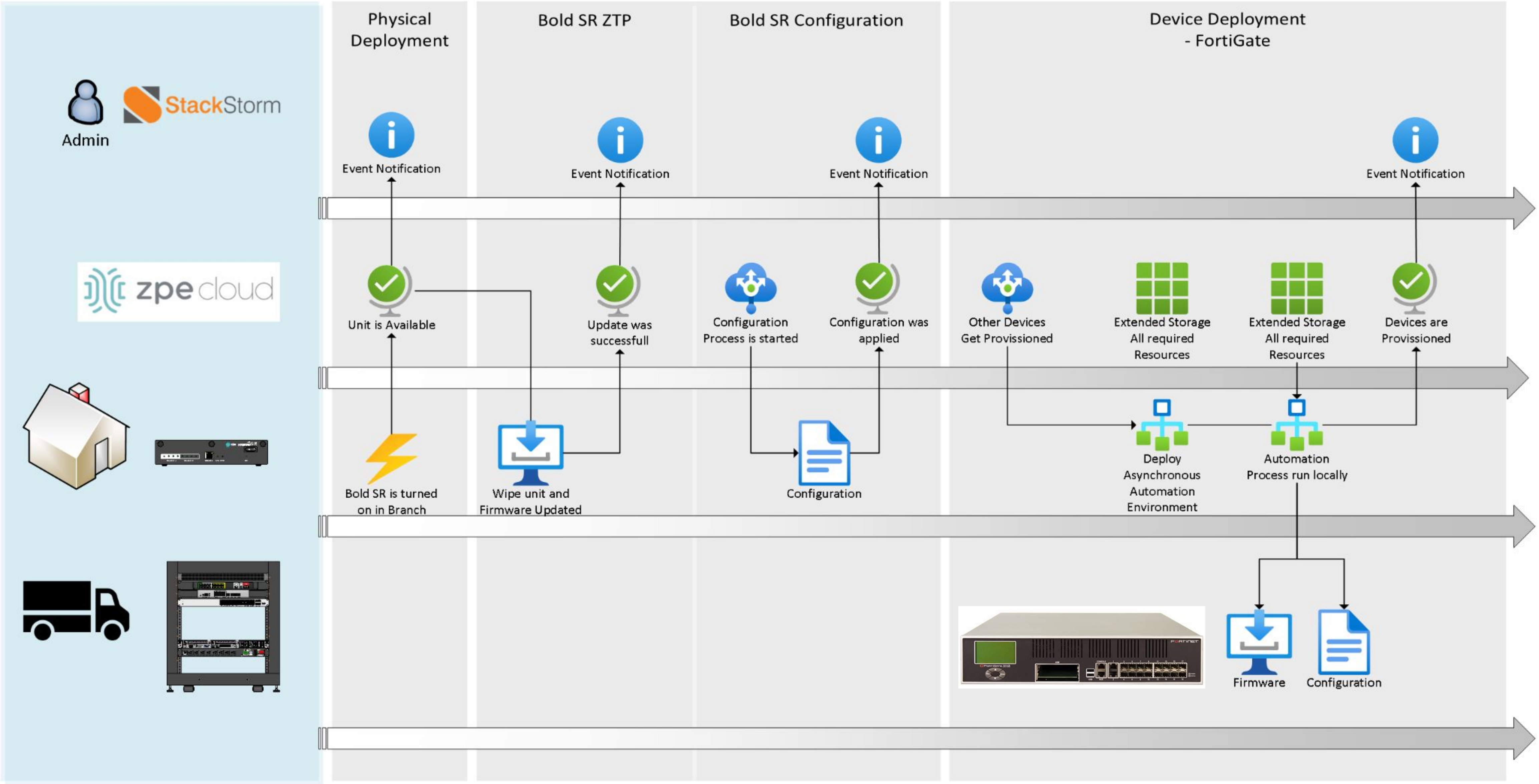
Intel® Network Builders ECOSYSTEM PARTNER
An Industry Leading Ecosystem
intel.



Branch Setup



Demo


Physical Deployment
Bold SR ZTP
Bold SR Configuration
Device Deployment - FortiGate
Admin
StackStorm
zpe cloud
Event Notification
Event Notification
Event Notification
Event Notification
Unit is Available
Update was successfull
Configuration Process is started
Configuration was applied
Other Devices Get Provisioned
Extended Storage All required Resources
Extended Storage All required Resources
Devices are Provissioned
Bold SR is turned on in Branch
Wipe unit and Firmware Updated
Configuration
Deploy Asynchronous Automation Environment
Automation Process run locally
Firmware
Configuration

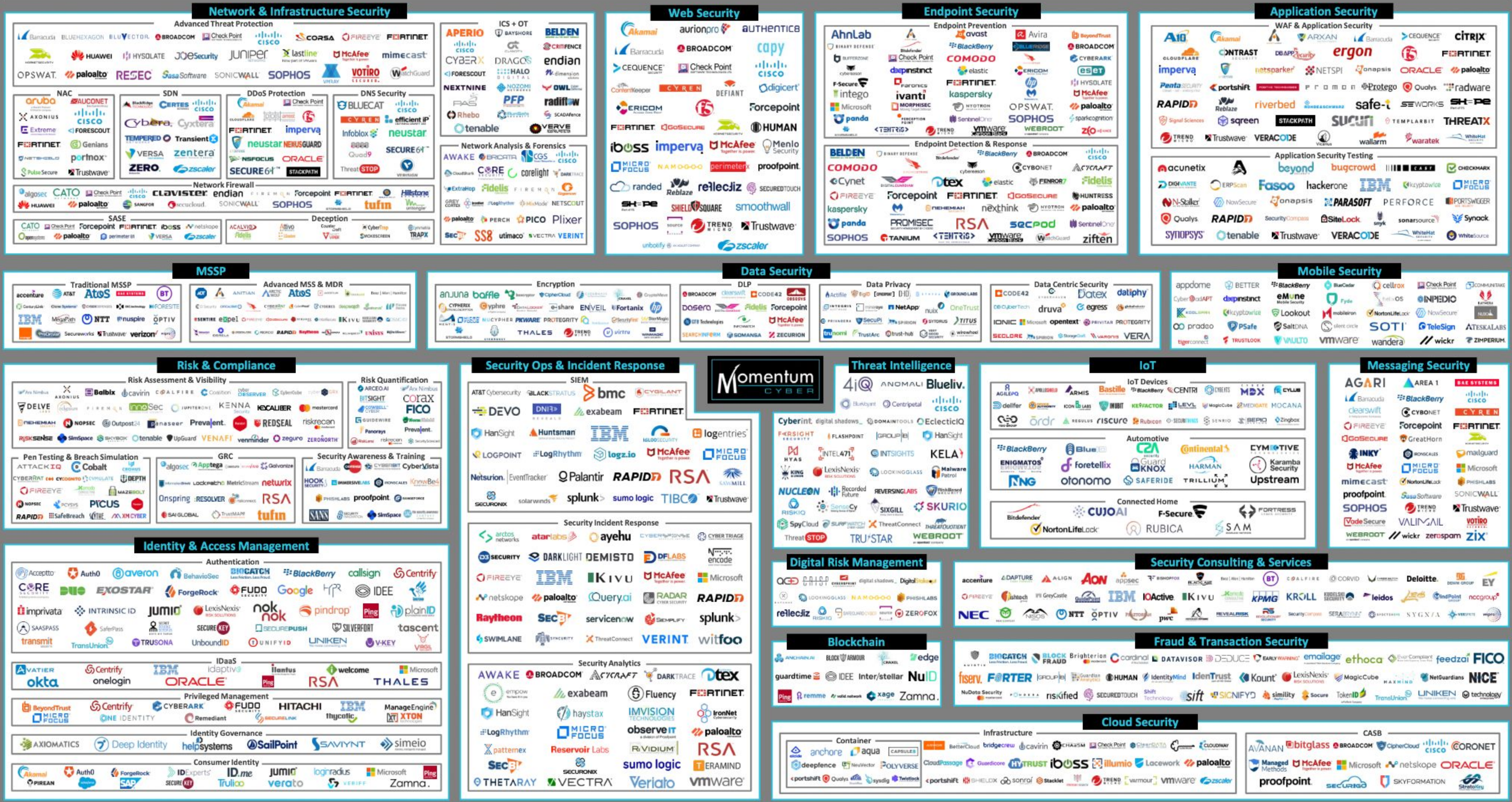
demoreel zpe®

SECURE EDGE DATACENTER DEPLOYMENT

Zero Pain Ecosystem
Launching Security Apps from ZPE's Platform

Rene Neumann
Director of Solution Engineering

CYBER SCAPE Too many products. Too many experts. Too many gaps. 2021



Network & Infrastructure Security
Advanced Threat Protection
ICS + OT
NAC
SDN
DDoS Protection
DNS Security
Network Analysis & Forensics
Network Firewall
SASE
Deception

Web Security

Endpoint Security
Endpoint Prevention
Endpoint Detection & Response

Application Security
WAF & Application Security
Application Security Testing

MSSP
Traditional MSSP
Advanced MSS & MDR

Data Security
Encryption
DLP
Data Privacy
Data Centric Security

Mobile Security

Risk & Compliance
Risk Assessment & Visibility
Risk Quantification
Pen Testing & Breach Simulation
GRC
Security Awareness & Training

Security Ops & Incident Response
SIEM
Security Incident Response
Security Analytics

Momentum CYBER

Threat Intelligence

IoT
IoT Devices
Automotive
Connected Home

Messaging Security

Identity & Access Management
Authentication
IDaaS
Privileged Management
Identity Governance
Consumer Identity

Digital Risk Management

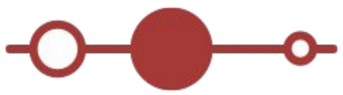
Blockchain

Security Consulting & Services

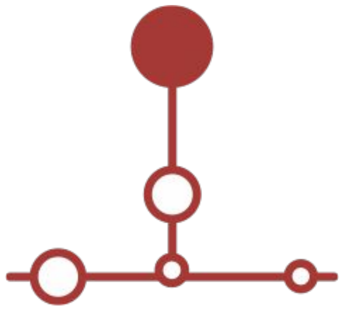
Fraud & Transaction Security

Cloud Security
Container
Infrastructure
CASB

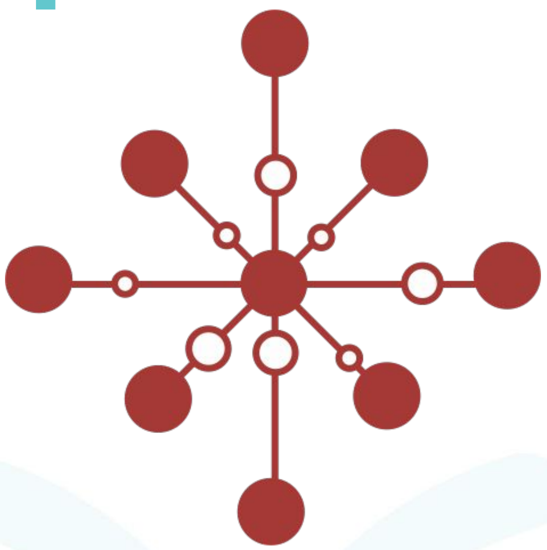
The Three Requirements of Running Security Apps



In Path of Traffic



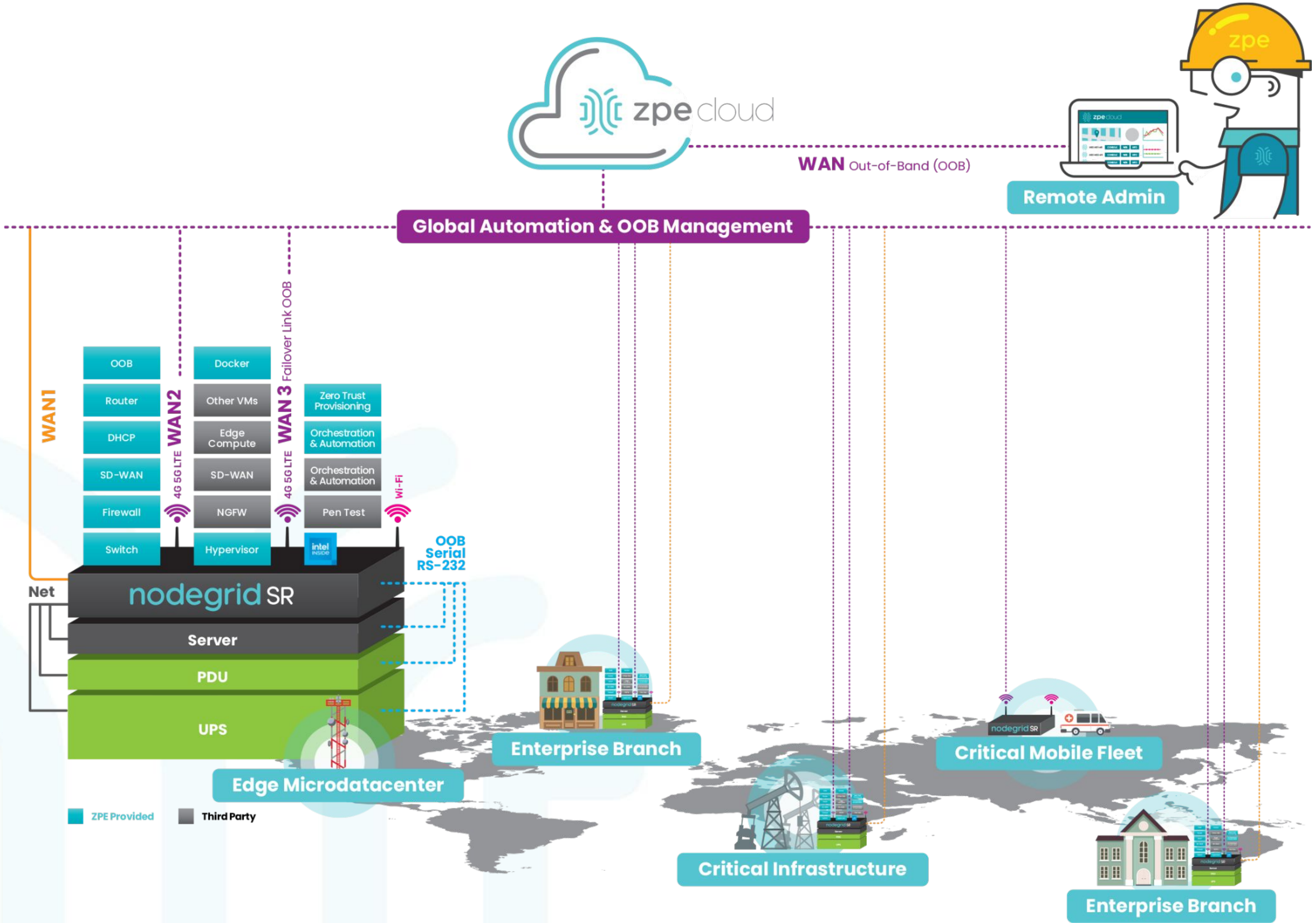
Insert Traffic



At All Locations

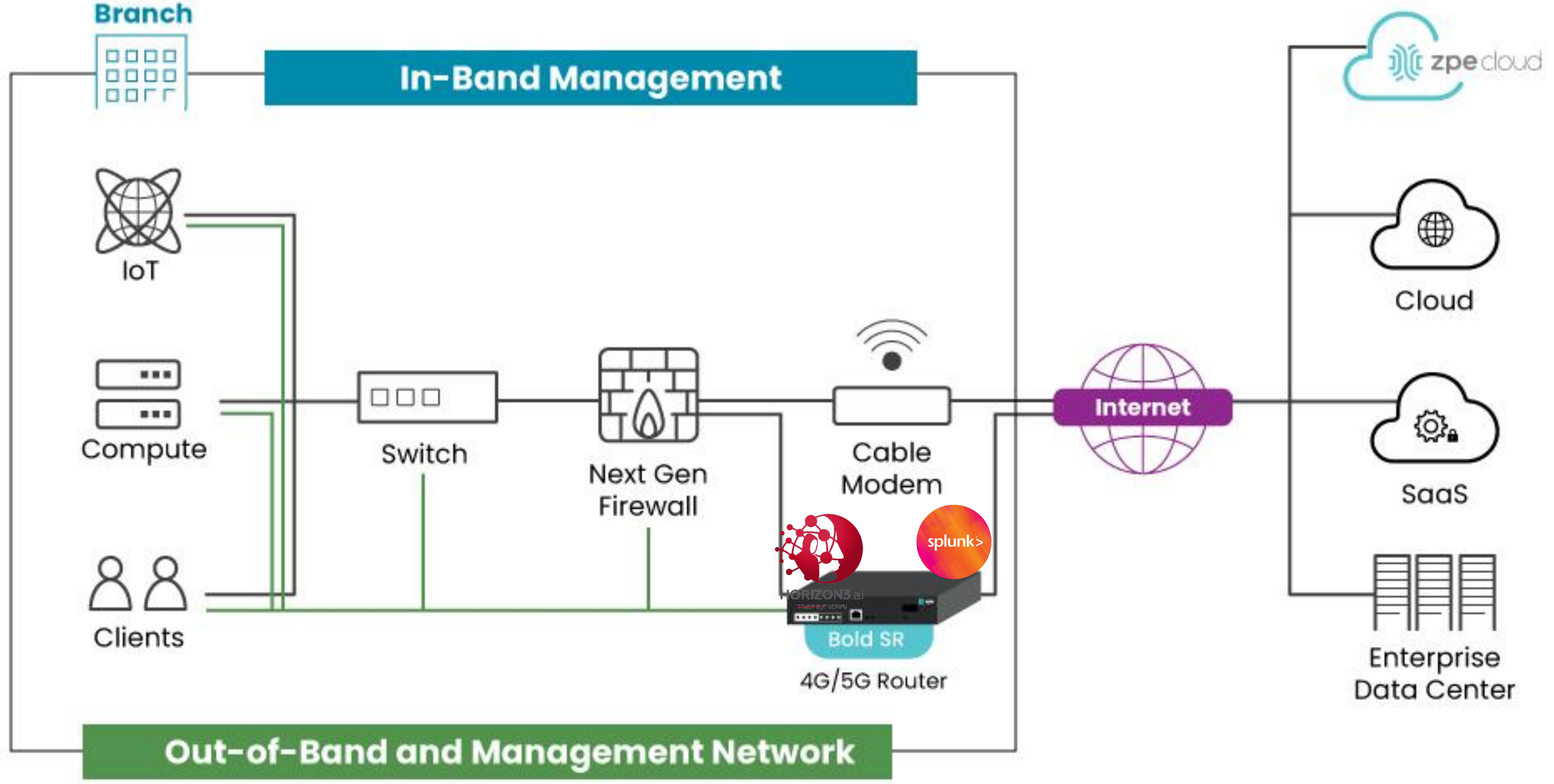
● Security App ○ Traffic

Launching Security Apps from ZPE Platform



info@ZPEsystems.com @ZPEsystems

Launching Security Apps from ZPE Platform



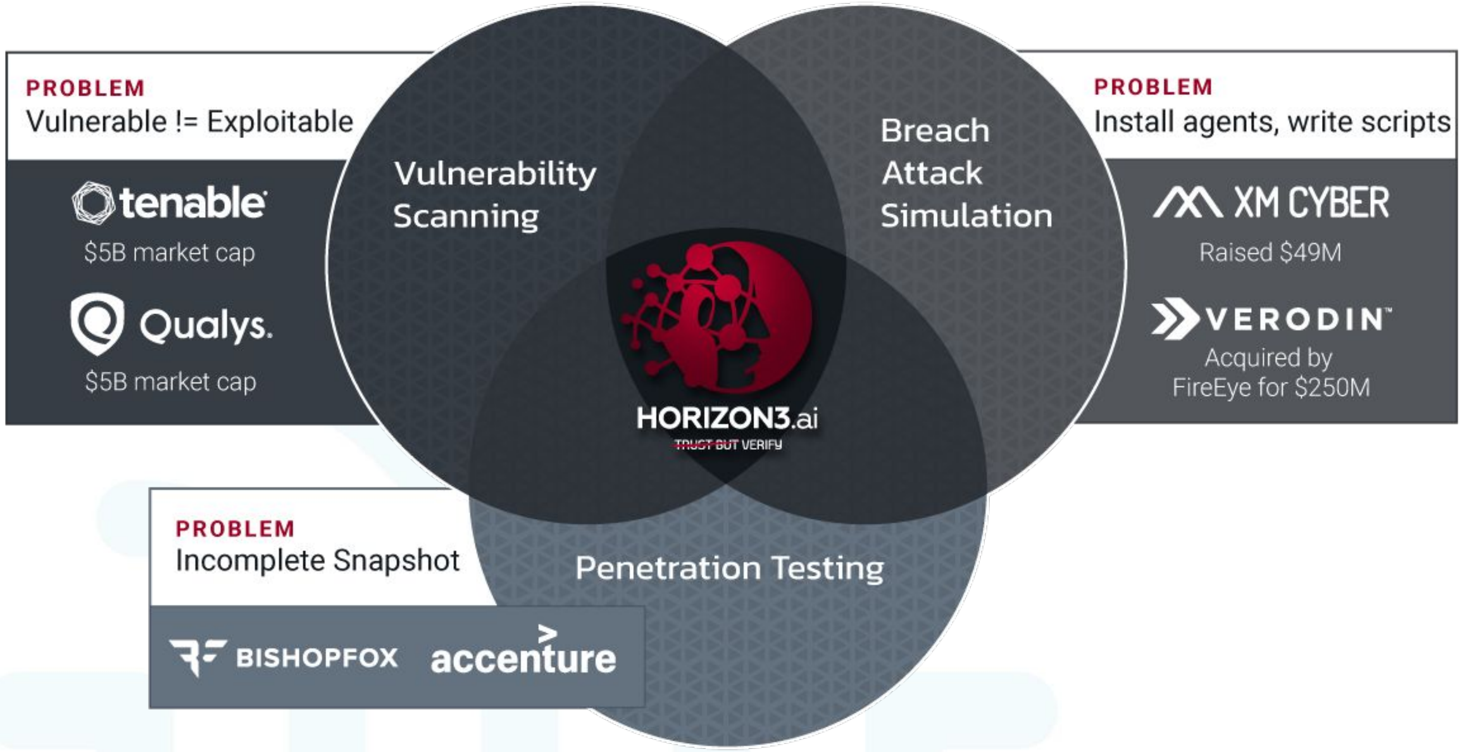
Security Apps

1. Autonomous PenTest Horizon3.ai
2. Additional Visibility XDR - Splunk
3. Event Driven Automation - StackStorm
4. ZTNA - Netskope

HORIZON3.ai splunk> StackStorm netskope

See latest prevalidated apps on website
https://www.zpesystems.com/prevalidated-virtualized-applications/

NodeZero from Horizon3.ai AUTONOMOUS PEN TEST



PROBLEM
Vulnerable != Exploitable

tenable
$5B market cap

Qualys.
$5B market cap

PROBLEM
Install agents, write scripts

XM CYBER
Raised $49M

VERODIN
Acquired by FireEye for $250M

PROBLEM
Incomplete Snapshot

BISHOPFOX accenture

Effort: Self-service, Agentless, 100% Autonomous

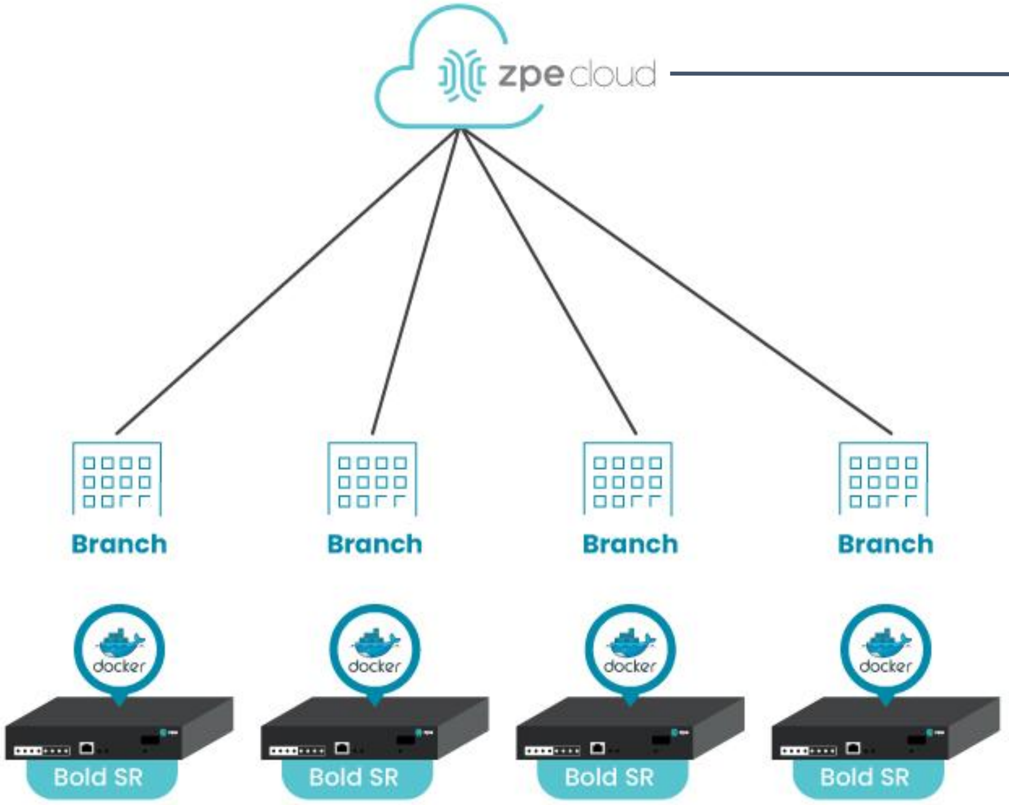
Speed: Hours NOT weeks

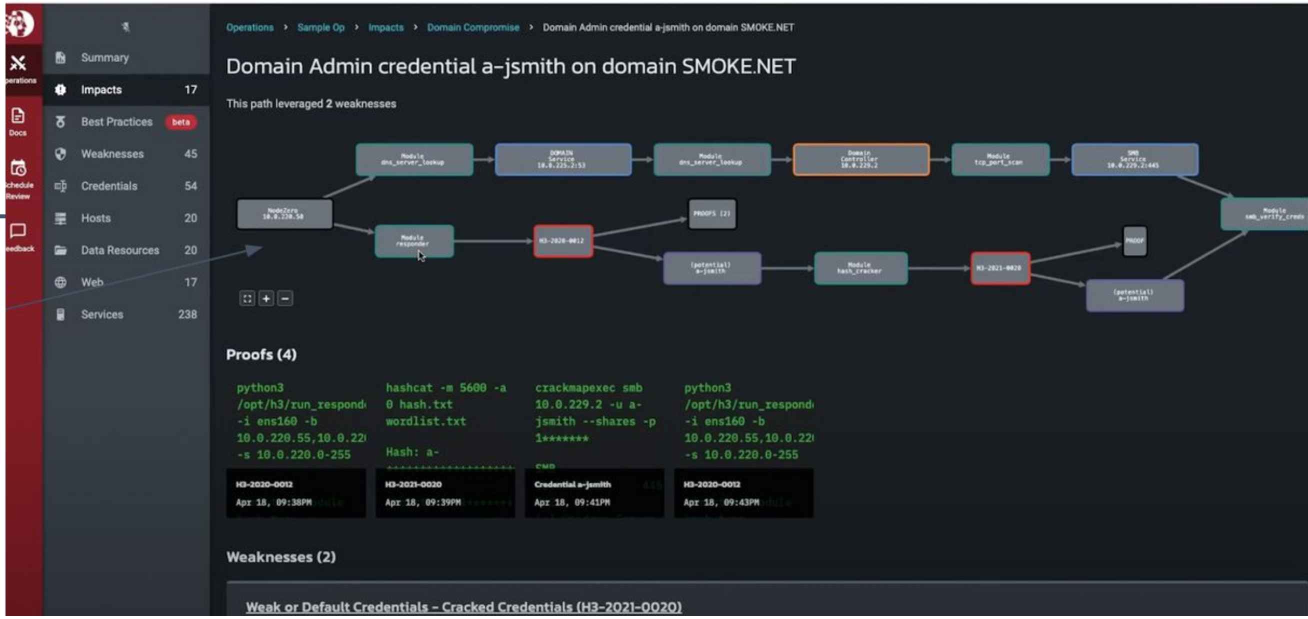
Accuracy: Proof + Path = No False Positives

Coverage: 100% of network

Frequency: Continuous

Autonomous Pen Test Horizon3.ai





Operations › Sample Op › Impacts › Domain Compromise › Domain Admin credential a-jsmith on domain SMOKE.NET

Domain Admin credential a-jsmith on domain SMOKE.NET

This path leveraged 2 weaknesses

Proofs (4)

```
python3
/opt/h3/run_respond
-i ens160 -b
10.0.220.55,10.0.22
-s 10.0.220.0-255
```

H3-2020-0012
Apr 18, 09:38PM

```
hashcat -m 5600 -a
0 hash.txt
wordlist.txt

Hash: a-
```

H3-2021-0020
Apr 18, 09:39PM

```
crackmapexec smb
10.0.229.2 -u a-
jsmith --shares -p
1*******

SMB
```

Credential a-jsmith
Apr 18, 09:41PM

```
python3
/opt/h3/run_respond
-i ens160 -b
10.0.220.55,10.0.22
-s 10.0.220.0-255
```

H3-2020-0012
Apr 18, 09:43PM

Weaknesses (2)

Weak or Default Credentials – Cracked Credentials (H3-2021-0020)

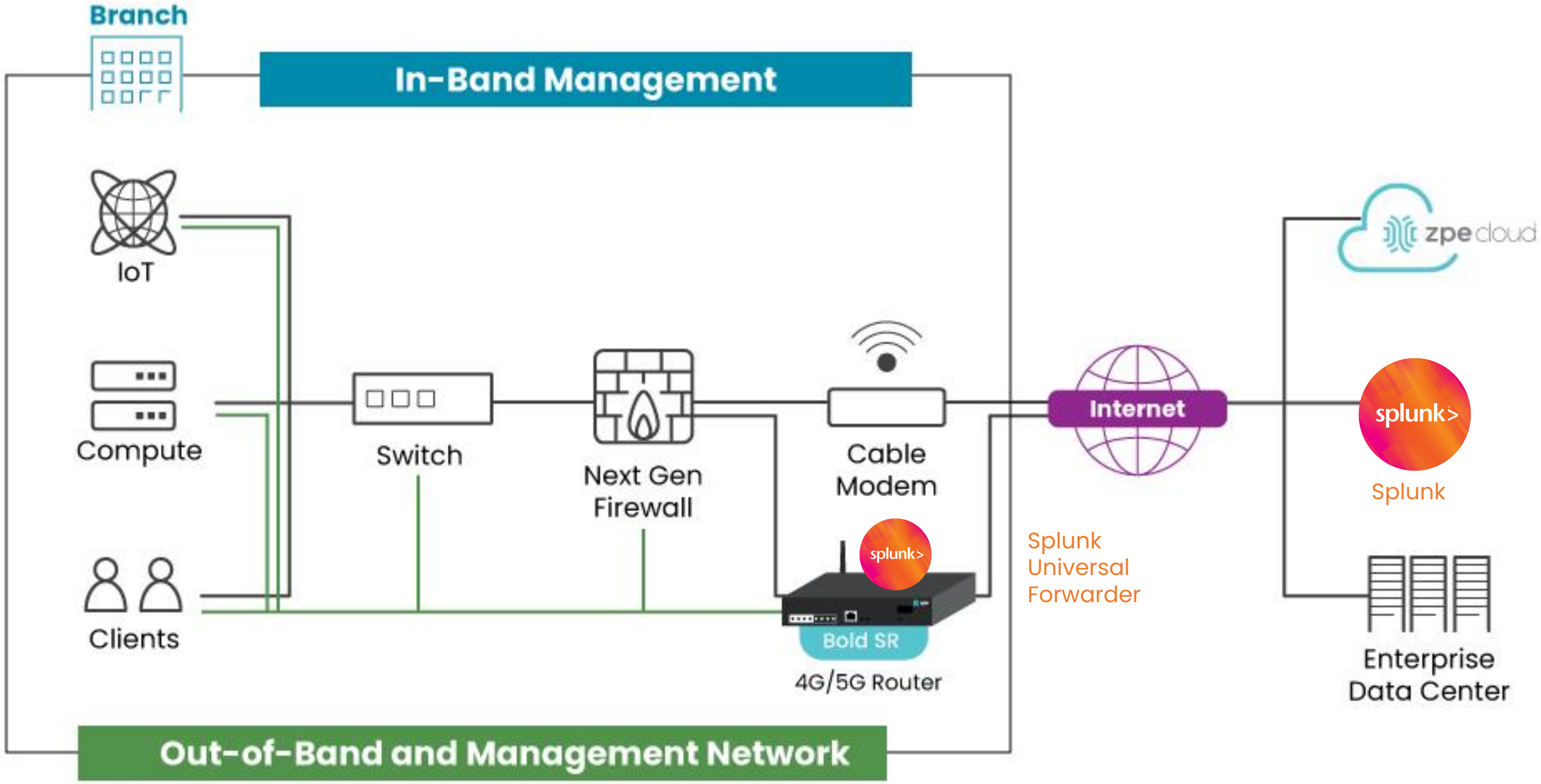
- Through ZPE Cloud, Autonomous Pen Tests can be scheduled
- Bold SR downloads latest Docker image
- Bold SR executes the PenTests
- Reports the results back to Horizon3.ai

demoreel zpe®

HORIZON3.AI

Additional Visibility XDR-Splunk

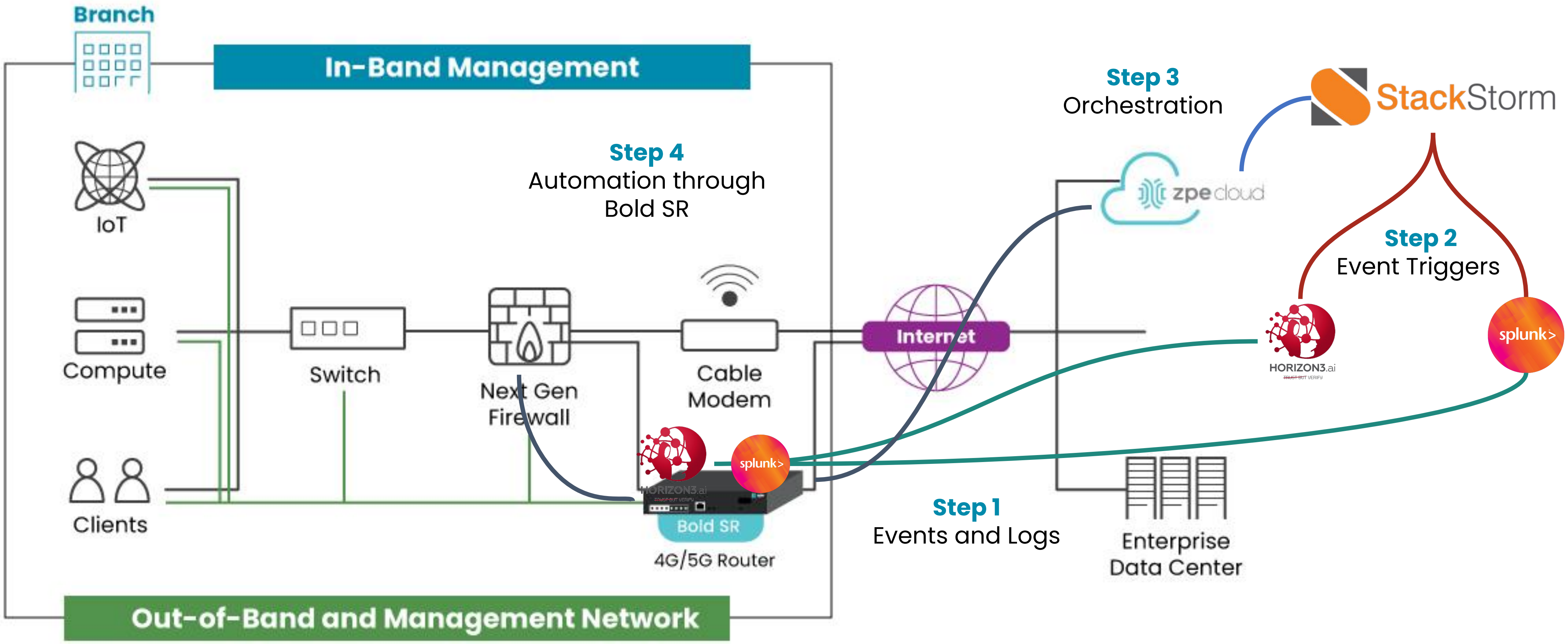
- **Splunk Universal Forwarder** is installed on Bold SR in each Branch
- All logs are locally collected and forwarded based on Splunk policies
- Gather additional logs like console logs
- Consistent and scale platform for all branches



demoreel zpe®

SPLUNK

Event Driven Automation Stackstorm



demoreel zpe®

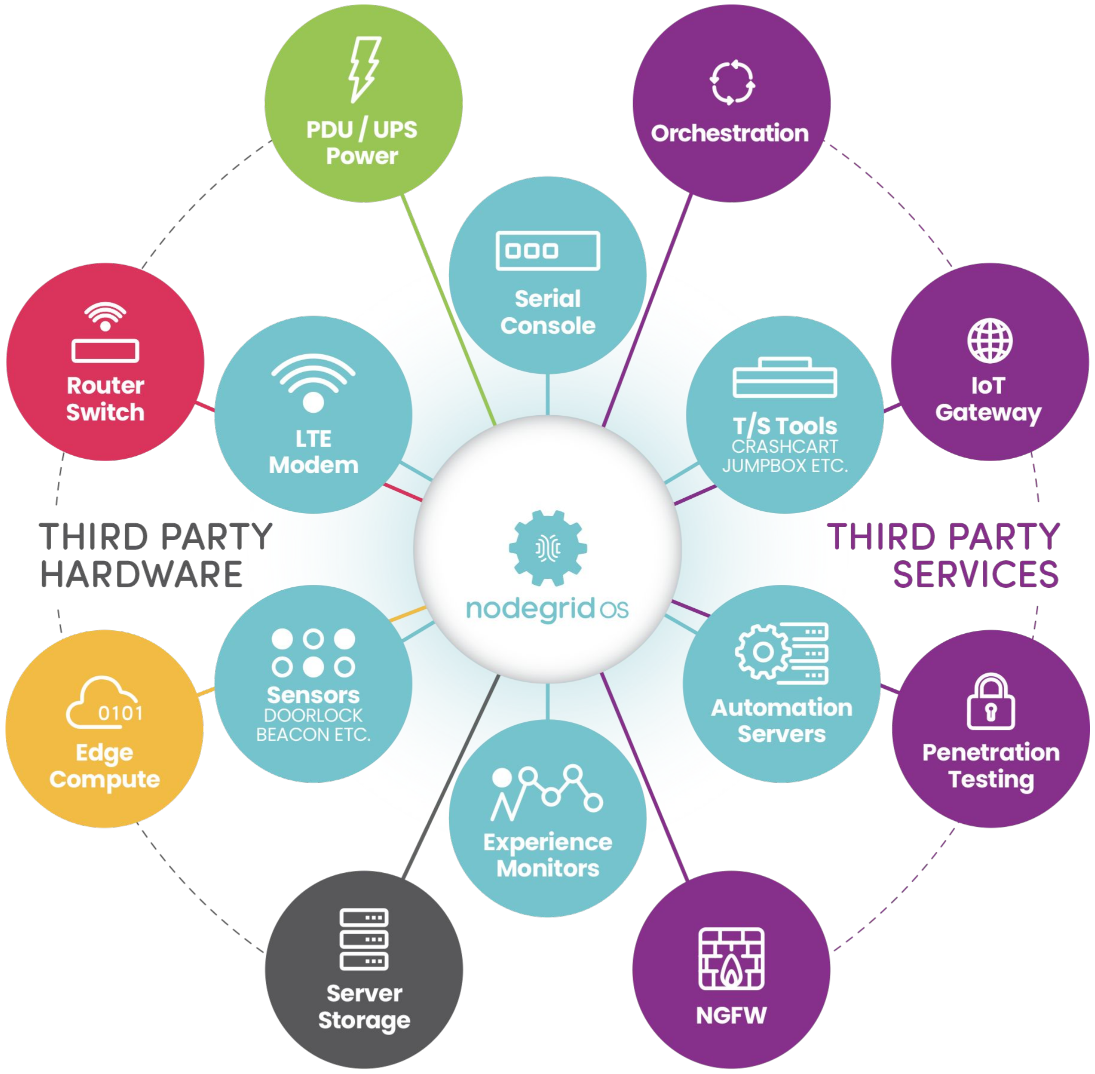
STACKSTORM

info@ZPEsystems.com **@ZPEsystems** zpe

Nodegrid Platform

Ideal choice for your cybersecurity deployments

- **Flexible** Nodegrid Platform can be utilised for most aspects of the test cycle like running **Horizion3.ai** or **Splunk**
- **Consistent Platform** Nodegrid platform can be used in all Enterprise environments, from Mega Data Center to Nano Data Centers at the Edge, providing a consistent platform, throughout the Enterprise
- **Automation Platform** Nodegrid provides the ideal automation platform for all aspects of the testing cycle, from testing all the way through to fixing



Zero Pain Ecosystem

🟦 ZPE Systems Scope

TRUSTED BY
6 OF THE TOP 10
MOST VALUABLE
GLOBAL TECH GIANTS

Contact Us

Sales
sales@zpesystems.com

General Information
info@zpesystems.com

Schedule a Demo
zpesystems.com/demo

ZPE Systems, Inc.

3793 Spinnaker Court
Fremont, CA 94538
United States

+1 844 497 3797
zpesystems.com