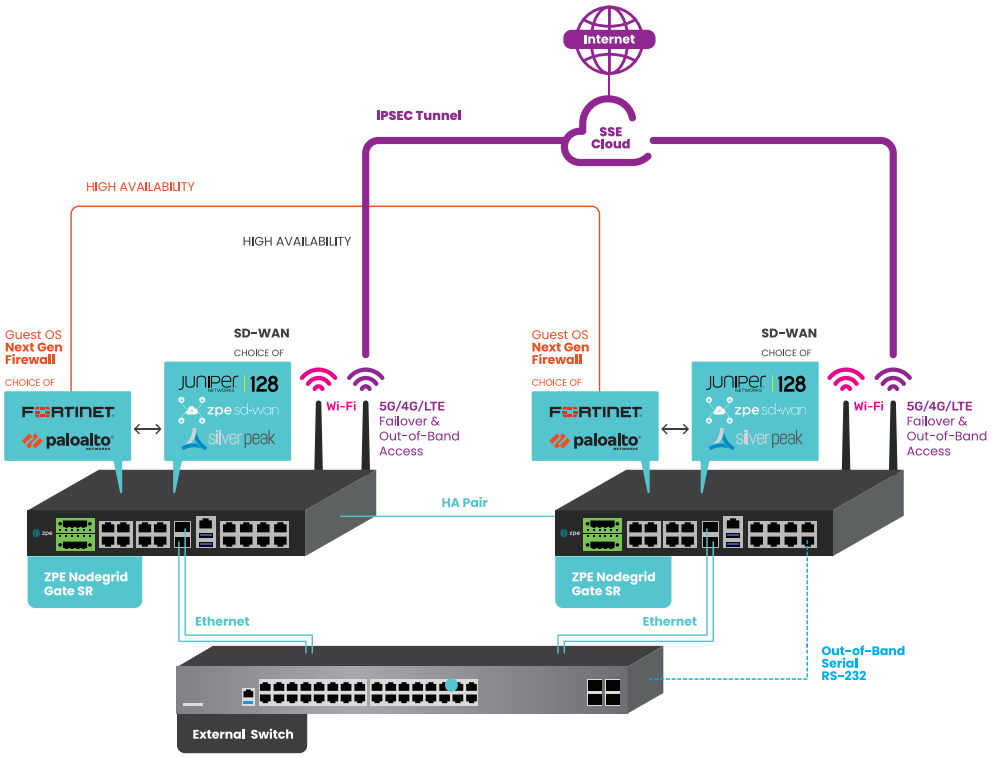
ZPE Systems' Services Delivery Platform: Deploy any app, any time, anywhere

Summary

Organizations struggle to manage the hundreds of products involved in enterprise security. Most NGFWs, SD-WAN, pen testers, and on-prem & cloud solutions require hardware platforms to be deployed with the rest of enterprise IT, which creates infrastructure sprawl. This hardware lock-in prevents IT from switching to other vendors and applications, while the technical overhead locks IT teams into performing tedious operational tasks — such as provisioning, installing, and orchestrating dedicated hardware — instead of enabling them to deliver services quickly and focus on providing business value.

ZPE Systems solves this with the Services Delivery Platform. This approach, which Gartner calls platform engineering, facilitates streamlined deployment, activation, and orchestration of services — when and where they are needed — via self-service capabilities and infrastructure automation. The Services Delivery Platform's open hardware and software directly host VMs, containers, apps, and automation solutions, enabling teams to provide business value through flexible, on-demand service delivery.



Problem - Operational friction delays service delivery

Enterprise IT is under pressure both from business demand and emerging cyber threats. To protect physical and virtual assets, the typical environment consists of hundreds of cloud and on-prem security solutions, cobbled together from a pool of more than 1,800 cybersecurity vendor options. These solutions, whether NGFWs, SD-WAN, or other apps and tools, must be deployed and orchestrated on physical hardware.

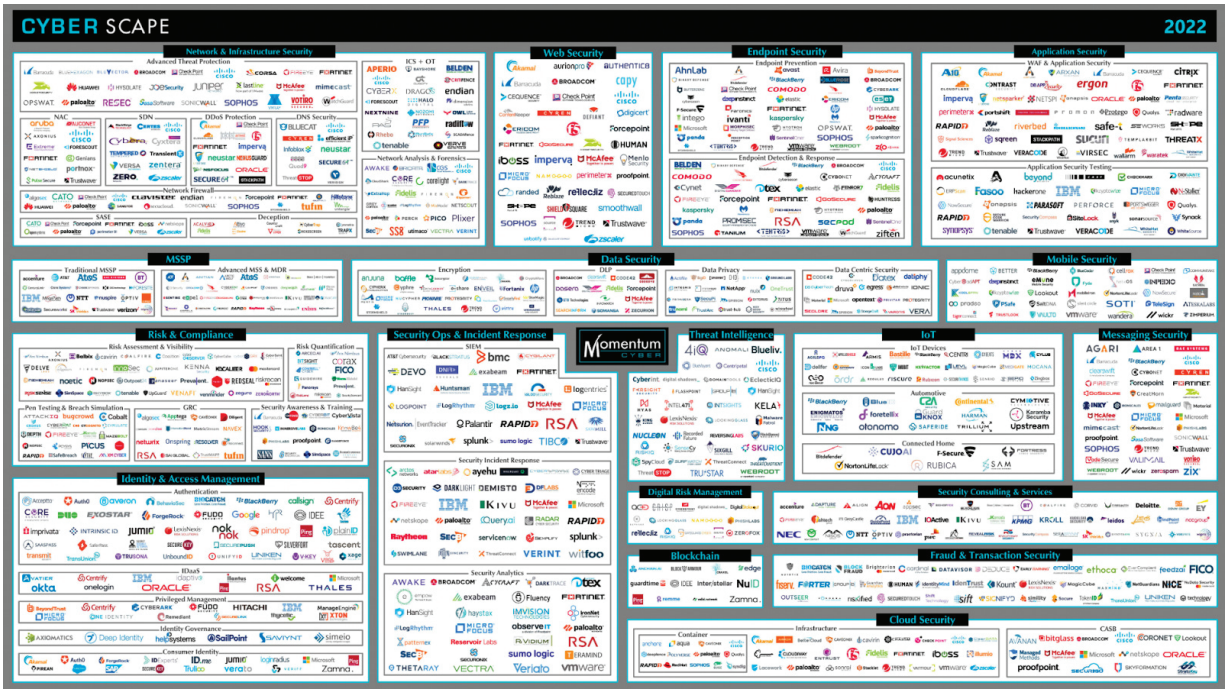


Image (Courtesy of The Momentum Cyberscape 2021): Admins are faced with delivering many services for enterprise IT operations.

Private cloud and on-prem infrastructure require dedicated hardware, additional servers, and operating systems on which to run security solutions. Even SASE — the concept of delivering networking and security via the cloud — requires branch offices to house physical hardware to serve as the application on-ramp.

Deploying these systems transforms IT into a complex machine, with many moving parts located at edge, branch, and data center locations. This infrastructure sprawl leads to operational friction, the buzzword for all of the tedious tasks associated with provisioning, deploying, configuring, and troubleshooting new service integrations. Operational friction becomes the focus of IT teams, which ultimately stalls the pace at which they can deliver services to generate revenue, recover from outages, or stop ransomware attacks.

Gap - Teams aren't equipped to accelerate delivery

The trouble is, teams are stalled by complexity and disjointed tools. There's no 'easy' button for deploying an SD-WAN solution, NGFW, SASE agent, or pen-testing client. Each comes with unique tools, management interfaces, and automation capabilities that require specific skills in order to be integrated into the rest of an already complex machine.

For example, teams implementing penetration testing need to answer questions like:

- Where do I install my pen test agent in remote locations?
- Is there a device I can connect to all the different VLANs that I need to scan?
- Can I secure the OS on this device and keep it up-to-date with security patches, so it doesn't become an attack surface?
- How can I manage a large fleet of these devices from a centralized location and keep them automatically updated?
- How can I then use this platform for other services so I can consolidate the hardware at branch locations?

Having to solve these challenges forces teams into inefficient delivery pipelines and managing the low-level infrastructure surrounding each service. The gap is that they lack a key mechanism that can both eliminate friction and accelerate service delivery.

Solution - Platform engineering enables on-demand service delivery

Gartner's concept of platform engineering fills this gap. This approach involves placing a platform of curated reusable tools, self-service capabilities, and automated infrastructure between teams and the services they need to deliver. The goal is to improve productivity and efficiency, with standardized tools and automated processes that allow teams to:

- Deploy any app, anytime, anywhere
- Switch/swap applications and services on-demand
- Manage distributed device fleets in a unified and centralized manner

With the pen testing example above, platform engineering gives teams a clear blueprint for successful service delivery, so they can focus on how to better secure their attack surface rather than on keeping surrounding IT operational.

"Today, non-expert end users are often asked to operate an assembly of complicated arcane services," says Paul Delory, VP Analyst at Gartner. "To help end users, and reduce friction for the valuable work they do, forward-thinking companies have begun to build operating platforms that sit between the end user and the backing services on which they rely."

The caveat to this approach is that it should be hosted on a proper management and orchestration network, which requires the right design pattern blueprint and expertise to build. This should also be hosted on hardware that is itself security hardened at the most basic levels to minimize the attack surface. These issues, along with a lack of best practices for building this infrastructure, prevent most teams from putting platform engineering into practice.

ZPE Systems' Services Delivery Platform Brings Platform Engineering to Life

Since 2013, ZPE Systems has worked with Big Tech to streamline service delivery. This led to the creation of best practices for out-of-band management and automation, as well as the development of powerful, open software and hardware. 6 of 10 top tech giants now use this Services Delivery Platform to deploy any app, anywhere, at any time, to help business:

- Generate revenue fast: Open integration with any app & automation tool enables push-button, end-to-end service delivery
- Reduce outage costs: Dedicated remote access allows instant service troubleshooting & recovery at any location
- Stop ransomware attacks: Encrypted hardware & automated patching minimize supply chain security risks and the attack surface
- Avoid vendor lock-in: The Services Delivery Platform enables IT to replace low-performing apps in just weeks versus waiting 3 to 7 years for hardware to become obsolete

ZPE's Services Delivery Platform allows teams to quickly deploy a resilient management network and the platform engineering component, both on a single, multi-function device.

First, the resilient, Double-RingTM management architecture is established. This is achieved through dedicated LAN and WAN links connected to ZPE's Nodegrid devices, which feature multiple interface types and modular expansion cards — from serial, ethernet, and USB, to IPMI, KVM, and others. Nodegrid devices include a secure root of trust, TPM 2.0, and encrypted disk to eliminate the physical attack surface and address supply chain security. This out-of-band control plane securely carries management traffic, removes the attack surface, shields devices from the Internet, and removes admin connectivity from relying on the main network.

This is the foundation of the Services Delivery Platform, enabling teams to efficiently deliver VMs, containers, and any choice of app via Nodegrid's multi-core Intel CPU and Linux-based Nodegrid OS. Wherever teams deploy Nodegrid, they can also leverage complete service activation and chaining through ZPE Cloud's zero touch provisioning. This extends automation and orchestration across environments and device types, allowing teams to standardize delivery of SASE, NGFWs, SD-WAN, and any on-prem or cloud solutions in their environment.

The Services Delivery Platform brings platform engineering to life so organizations can eliminate operational friction, accelerate service delivery, and increase IT's productivity.

Run pen tests anytime, anywhere with Horizon3 and ZPE Systems

ZPE makes it easy to deliver any app, anytime, anywhere, so you can keep every site secure. See how the Services Delivery Platform enables comprehensive, daily penetration testing with Horizon3.ai's NodeZero application.

Download the Horizon3 and ZPE solution guide today.