Automated Infrastructure Patching for Ransomware Defense

Summary

Ransomware attacks continue to be successful because organizations often leave infrastructure unpatched. IT teams sit on the latest patches and updates from their solution vendors, which exposes infrastructure for the taking and leaves it vulnerable to weaponized ransomware, increased cyber insurance fees, and prolonged recovery efforts. Why is this normal? Because IT teams lack best practices for applying patches, turning the Friday-night upgrade into a scary job that could break the entire system.

ZPE Systems solves this with the reference architecture for automated infrastructure patching, an architecture recommended by Gartner. This involves creating a dedicated control plane via out-of-band infrastructure, which enables teams to securely patch devices and automate recovery and rollback in case of issues. Big Tech uses this best practice to automate patching and recover systems in case of errors.

Problem

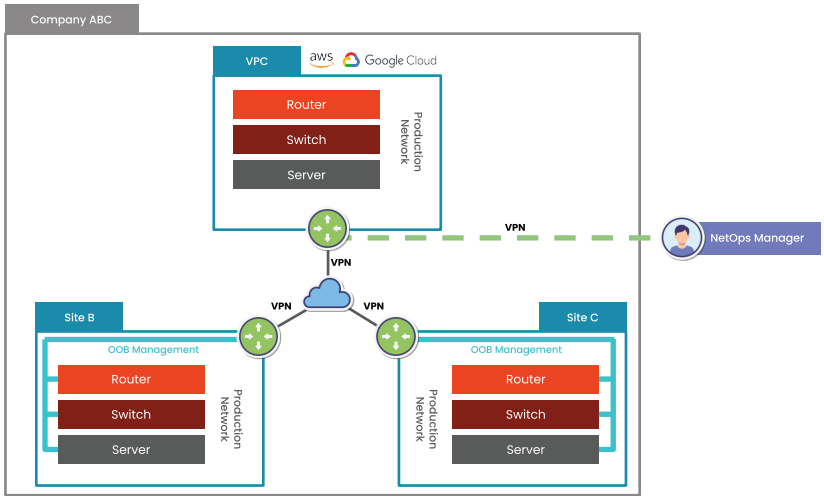
Cybersecurity is a $155 billion industry, giving organizations thousands of sophisticated products to choose from. Why, then, are attacks expected to cause $10.5 trillion in damages by 2025? Today's average attack costs $3.5M, while this expense is expected to increase and soon fall outside of cyber insurance coverage. The problem lies in unpatched infrastructure.

Organizations typically deploy many different security products with the intent of reinforcing their defenses. But these products can be bypassed by gaining access to servers, routers, and switches that remain unpatched and vulnerable. Frequent patching is necessary to close the attack surface and address CVEs, but this is time consuming without the right design pattern. Administrators would rather not risk collapsing operations with firmware/software updates, so many portions of infrastructure are left unpatched, creating a porous, growing attack surface.

Gap - Patching is risky business

Admins know that patching can produce errors (and patches often include errors themselves) capable of causing major outages. From crashing critical devices, to taking digital services completely offline, IT teams are well aware of the risks involved in deploying patches — and how these risks are directly tied to business revenues and costs. One patch that causes hanging firmware, applied to 100 sites, results in at least 100 truck rolls and thousands of unhappy customers.

For admins, patching lacks best practices and is therefore a gamble. They cannot positively answer the question, "If this breaks my infrastructure, can I immediately recover?" A knowledge gap exists: admins see no other method than to deploy patches directly to their production infrastructure, with no way to roll back to a safe configuration.



Solution - A dedicated automation infrastructure for automated patching

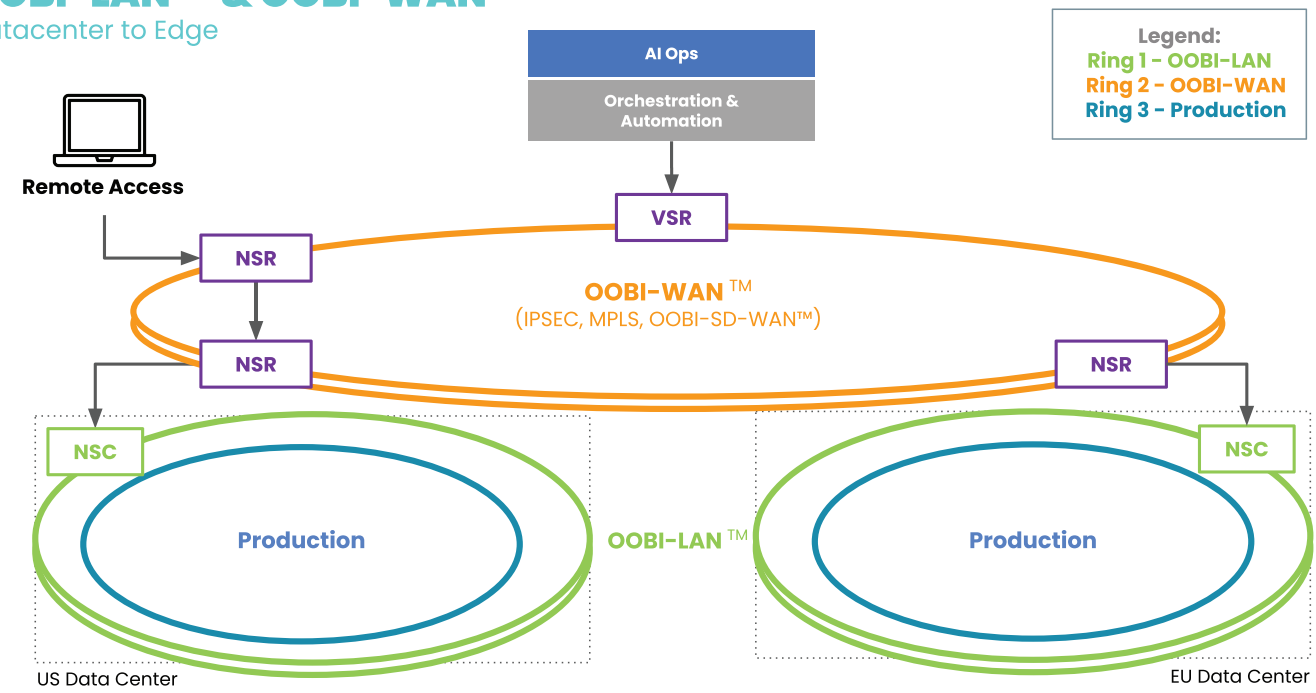
To fill this gap, admins need confidence in their ability to apply patches, but more importantly, they need the peace of mind knowing they can recover quickly in case of issues. These can stem from typos or config errors that knock devices offline, or from issues that are beyond their control, as experienced with 2022's FortiOS 7.0 CVE that left organizations scrambling to roll back to a more secure FortiOS 6.2.

The solution is to deploy a dedicated automation infrastructure that does not rely on the production environment and which provides access to all management interfaces, including console interfaces for automation. Gartner has recognized this out-of-band approach as the correct design pattern for applying frequent, automated patches. They call this the control plane infrastructure for production gear. This allows organizations to constantly shrink their attack surface in defense against emerging threats. But most importantly, this serves as the isolated automation infrastructure that allows admins to safely perform one-click rollback and recovery.

The one drawback is that this architecture is often tedious and time-intensive to set up, requiring dedicated devices from different vendors, manual VPN tunnels, and some exposure to the public Internet.

Secure Out-of-Band Infrastructure Rings: OOBI-LAN™ & OOBI-WAN™

Datacenter to Edge



ZPE Systems automates management infrastructure setup

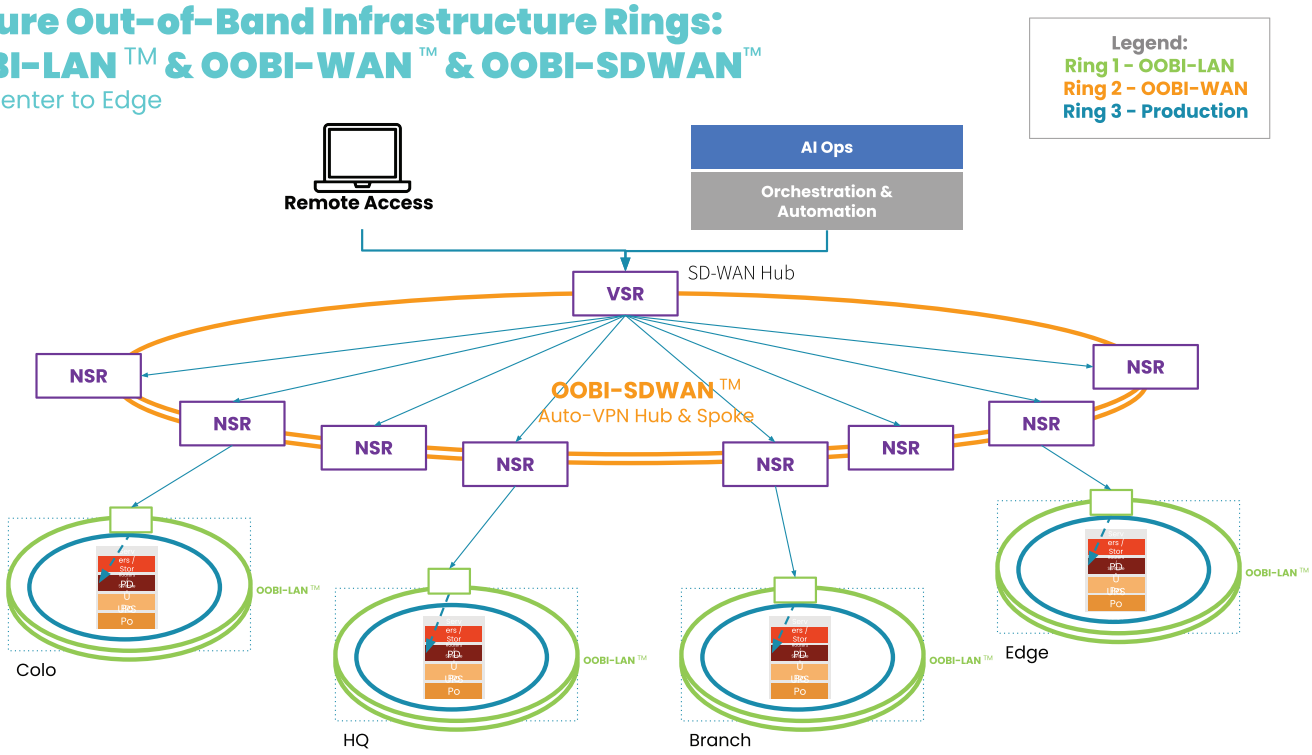
Over the past decade, ZPE Systems has closely collaborated with Big Tech to blueprint a new best practice that makes this management infrastructure more resilient and easy to deploy. Six of ten top tech giants and hundreds of enterprises in every industry now rely on this best practice to:

- Generate revenue: Automated setup & recovery ensure business continuity
- Reduce costs: Dedicated remote access eliminates expensive truck rolls
- Eliminate risk: Automated patching stops ransomware & allows safe rollbacks
- Reduce Downtime: Through automated configuration changes and fully integrated automatic recovery and rollback

ZPE enables a Double-Ring™ management architecture with dedicated LAN and WAN links for resilience.

Secure Out-of-Band Infrastructure Rings: OOBI-LAN™ & OOBI-WAN™ & OOBI-SDWAN™

Datacenter to Edge



Additionally, this out-of-band infrastructure (OOBI) is deployed and set up automatically using SD-WAN, without exposing devices to the Internet.

At the push of a button, ZPE's Virtual Services Router (VSR) sets up auto VPN hub-and-spoke connections to the Nodegrid Services Routers (NSRs) distributed to an organization's various sites. This OOBI-SDWAN provides the dedicated architecture for both remote access to and automation of WAN and LAN infrastructure.

Using this separate control plane gives admins a dedicated path through which to automatically apply patches using Ansible or other automation tools and also to gain remote access in case recovery is required. Administrators get the peace of mind knowing that they can patch against ransomware while having a safety net to instantly undo business-impacting issues.

See how Vapor® IO achieves true lights-out management

Vapor IO is re-architecting the internet with micro edge data centers. See how they automated full-site deployments and ongoing infrastructure management using ZPE's best practices. ***Download the full Vapor IO case study.***

"Nodegrid keeps our costs down and extends everyone's capabilities. The automation lets our support teams do specialized jobs, so our engineers can devote more time to delivering customer value." — Frank Basso, EVP of Operations, Vapor IO

zpe