Edge Pen Testing: Run Horizon3 on ZPE Systems' Services Delivery Platform

Summary

Enterprise IT teams struggle to secure their environments. One proven approach is for teams to attack their own network, a process called security penetration testing, which is executed externally or internally of the network and extends to all areas of internal networks. The goal is for teams to discover their level of security at remote locations, branch offices, affiliate locations, and all VLANs, to ensure third-party or insider attacks do not propagate to critical digital assets.

The main challenge is that pen testing requires a physical platform to sit at these satellite locations and that can execute the test. This platform must be able to host the pen test application, be managed as a fleet, and be security hardened (signed OS, CVE patching) to safely sit on VLANs without itself becoming an attack vector.

ZPE Systems' Services Delivery Platform and Horizon3.ai's NodeZero™ automated penetration test solution fills these gaps. This joint solution simplifies execution of internal pen tests, automates scheduling of retests, reduces pen test efforts to hours, makes tests repeatable, and expands their scope to cover all IT infrastructure at every location. This solution improves security while reducing operational costs, as it can easily integrate into existing processes to automate patching and configuration management.

Problem - Cybersecurity requires a proactive approach

Many enterprises struggle to protect their IT environments, because traditional security methods can't keep up with today's cybersecurity threat models. McKinsey research explains that approaches to IT security and processes are changing from a maturity-based approach to a risk-based or "proactive cybersecurity" approach.

This proactive approach calls for reducing detection and response times, and embedding security throughout to achieve "security by design." Penetration tests are a valuable tool to help protect IT environments. However, there are some inherent weaknesses that make traditional pen tests difficult to incorporate as part of this proactive approach.

Gap - Pen tests are slow, expensive, and risky

Penetration tests are vital in assessing a company's external and internal threat landscape. But traditional pen tests come with some significant gaps:

- Slow: Most pen tests are performed manually. This is a time-consuming process that can take days or weeks, depending on the scope and environment.
- Expensive: Pen tests are costly due to the required expertise and manual work.
- Limited Scope: Because pen tests require plenty of time and money, they are often limited in scope.
- Limited Reach: To be effective, pen tests need to be run from all internal locations, which is often prohibitive in terms of logistics.
- Risk of Downtime: If the scope is not well defined, pen tests are likely to cause downtime, unexpected outages, and customer dissatisfaction.
- Project Based: Due to the expertise and costs involved, pen tests are performed as part of a project, such as putting a new solution into production. This ignores ongoing system changes and the dynamic, ever-evolving threat landscape.

Solution – Fast, frequent, and dependable pen tests

In order to support a proactive cybersecurity approach, enterprises must be able to perform penetration tests quickly, frequently, and across their infrastructure — including to edge locations. This requires a hosting platform that accommodates:

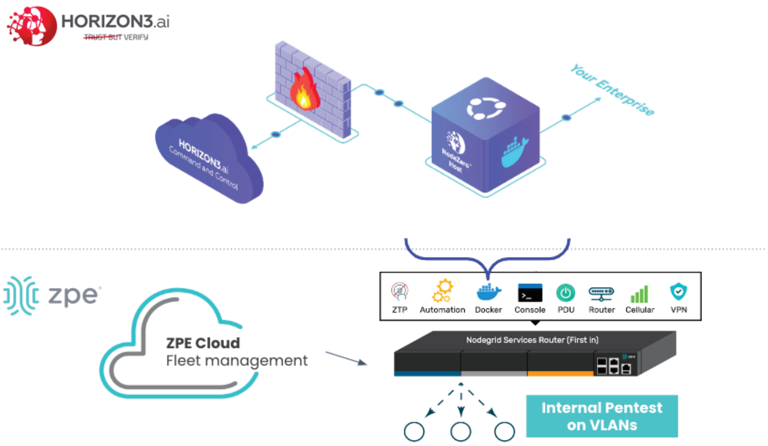
Speed: Attackers exploit new vulnerabilities in hours or days, which means enterprises need penetration tests that they can deploy quickly.

- Repeatability: Misconfigurations make up roughly 60% of all vulnerabilities, which means pen tests must be repeatable to assess config changes and ensure new vulnerabilities haven't been exposed.
- Expanded Scope: Phishing is the most common attack vector and leads to lateral movement. Combined with an increase of over 59% of shadow IT in the last few years, it's imperative that pen tests cover all IT management and operations within an organization. The hosting platform serves as a starting point to deploy global pen tests.
- Easy Recovery: Pen tests and active scanning can cause outages. Enterprises must be able to recover rapidly using automated methods.
- Process: Adopting a proactive approach means making security scans part of the change, deployment, and development processes. Enterprises need pen tests that they can automate as part of these processes.

ZPE Systems & Horizon3 automate pen testing across the enterprise

ZPE Systems' Services Delivery Platform and Horizon3.ai's NodeZero™ fill all of the gaps left by traditional penetration tests. This joint solution is easy to deploy and delivers full automation, allowing enterprises to integrate fast, repeatable pen testing into daily operations and change management processes. Enterprises can now achieve a proactive cybersecurity approach that incorporates pen testing.

ZPE's Services Delivery Platform directly hosts the NodeZero application and can automatically deploy and perform pen tests from any Type 1 hypervisor such as VMware or Linux KVM, or from a container platform. Tests take from an hour to a few hours based on the scope of the test, and reports are automatically provided at the end.



The Services Delivery Platform, which consists of the Nodegrid™ SR family of appliances and ZPE Cloud, is the ideal platform to host NodeZero. This joint solution solves the challenges associated with scope and recoverability, as Nodegrid devices come in form factors that fit any location, from industrial sites and warehouses, to retail, edge, and IoT environments. Nodegrid provides hardware-level security with encrypted disks, TPM 2.0, and a fully-signed Nodegrid OS.

Nodegrid natively provides out-of-band and virtualization capabilities, creating the infrastructure management and automation environment. This allows NodeZero to run in any location, enables reliable and rapid recovery when needed, and accommodates automatic pen test scheduling via ZPE Cloud.

Together, the Services Delivery Platform hosting NodeZero provides these benefits:

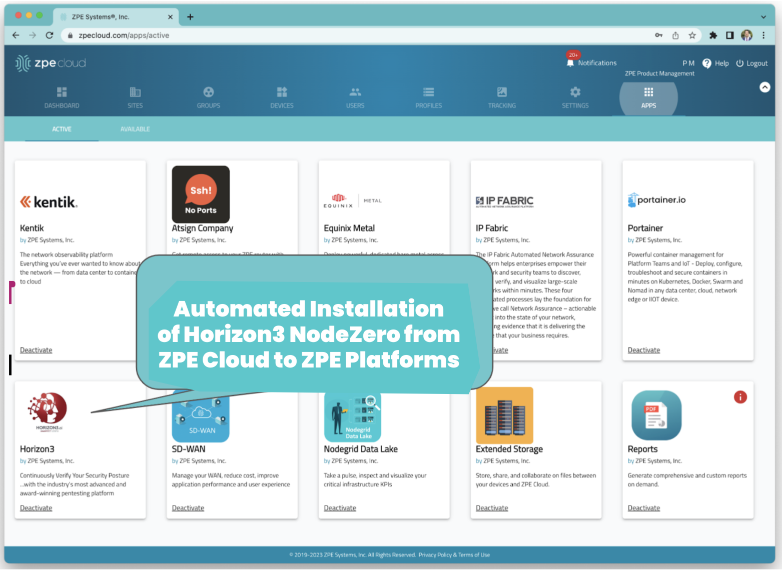
- Speed: NodeZero reduces pen testing times to mere hours, and gives a current view of the threat landscape. Enterprises can perform tests daily or weekly to maintain a proactive security posture.
- Repeatability: NodeZero with Nodegrid and ZPE Cloud make automated, repeatable pen testing possible. The API-first approach allows enterprises to clearly define the scope of their tests and reuse this scope when and where it's needed. They can keep test costs down, while gaining the ability to assess how planned and unplanned changes impact overall security.
- Expanded Scope: Enterprises can run NodeZero penetration tests on any Nodegrid device, giving them the freedom to expand this security to any location and environment. This expanded scope reduces blind spots created through shadow IT and misconfigured solutions, and simplifies operational efficiency. IT teams can deploy and test their global fleet from a single platform.
- Easy Recovery: ZPE's Services Delivery Platform provides a complete infrastructure for automation and management. If an attack, misconfiguration, or pen testing mistake occurs, IT teams can automatically patch and recover via fully independent management plane. This reduces operational costs and recovery times.
- Process: By enabling enterprises to run consistent, repeatable penetration tests with little effort, this joint solution can be fully integrated into change management and development processes. This ensures that new vulnerabilities are detected and resolved quickly, to create an IT environment that's proactively and holistically secure.

ZPE Cloud also eliminates the logistical challenges and security risks associated with preconfiguring devices to run pen tests. Teams no longer need to perform repeat work that increases the chance of misconfigs or errors, and they don't need to risk preconfigured device info being intercepted. They can deploy a fleet of factory-default Nodegrid devices, which upon booting up will connect to ZPE Cloud. From there, teams can automatically install NodeZero and run pen tests across their fleet simply by selecting NodeZero from the ZPE Cloud app store. This makes it easy to run pervasive, enterprise-wide testing from a centralized platform.

Get hands-on with NodeZero & the Services Delivery Platform

ZPE Systems' Services Delivery Platform and Horizon3.ai's NodeZero application help you address the modern threat landscape. Deploy this joint solution at any location to run fast, reliable pen tests and achieve a proactive security posture.

Protect your organization's IT environments — from core to edge — with ZPE Systems and Horizon3. Set up your personalized demo or POC at zpesystems.com/contact



Kentik
by ZPE Systems, Inc.
The network observability platform Everything you've ever wanted to know about the network — from data center to containe to cloud
Deactivate

Atsign Company
by ZPE Systems, Inc.

Equinix Metal
by ZPE Systems, Inc.

IP Fabric
by ZPE Systems, Inc.
The IP Fabric Automated Network Assurance ...rm helps enterprises empower their ...k and security teams to discover, ... verify, and visualize large-scale ...ks within minutes. These four ...ated processes lay the foundation for ...e call Network Assurance – actionable ... into the state of your network, ...ng evidence that it is delivering the ... that your business requires.

Portainer
by ZPE Systems, Inc.
Powerful container management for Platform Teams and IoT - Deploy, configure, troubleshoot and secure containers in minutes on Kubernetes, Docker, Swarm and Nomad in any data center, cloud, network edge or IIOT device.
Deactivate

Horizon3
by ZPE Systems, Inc.
Continuously Verify Your Security Posture ...with the industry's most advanced and award-winning pentesting platform
Deactivate

SD-WAN
by ZPE Systems, Inc.
Manage your WAN, reduce cost, improve application performance and user experience
Deactivate

Nodegrid Data Lake
by ZPE Systems, Inc.
Take a pulse, inspect and visualize your critical infrastructure KPIs
Deactivate

Extended Storage
by ZPE Systems, Inc.
Store, share, and collaborate on files between your devices and ZPE Cloud.
Deactivate

Reports
by ZPE Systems, Inc.
Generate comprehensive and custom reports on demand.
Deactivate

© 2019-2023 ZPE Systems, Inc. All Rights Reserved. Privacy Policy & Terms of Use

Automated Installation of Horizon3 NodeZero from ZPE Cloud to ZPE Platforms