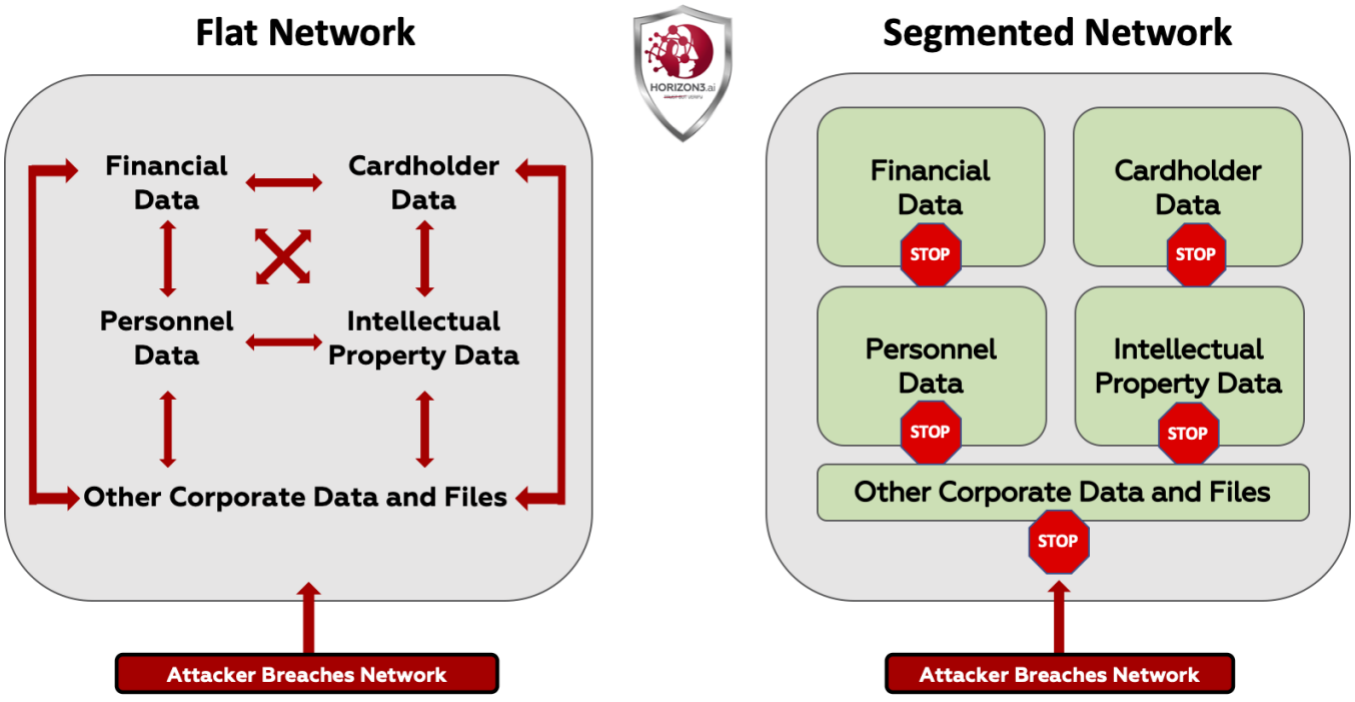
info@Horizon3.ai
www.Horizon3.ai
LinkedIn: Horizon3.ai
Twitter: @Horizon3ai

Network Segmentation Can Help You Move from Compliance to Security

A flat network, where everything is directly connected to everything else, makes security much more difficult. If an attacker breaches the network, they have access to everything, including sensitive data. And attackers **will** breach the network. Network segmentation gives you the power to limit the blast radius and the resulting damage of such an attack.



Better, Faster, Cheaper and Continuous Compliance and Security

Horizon3.ai provides Automated Pen Testing as a Service (APTaaS) with **NodeZero**, a fully automated cyber attacker that emulates the behavior of real-world attackers and delivers better, faster, cheaper and continuous compliance and security assessments.

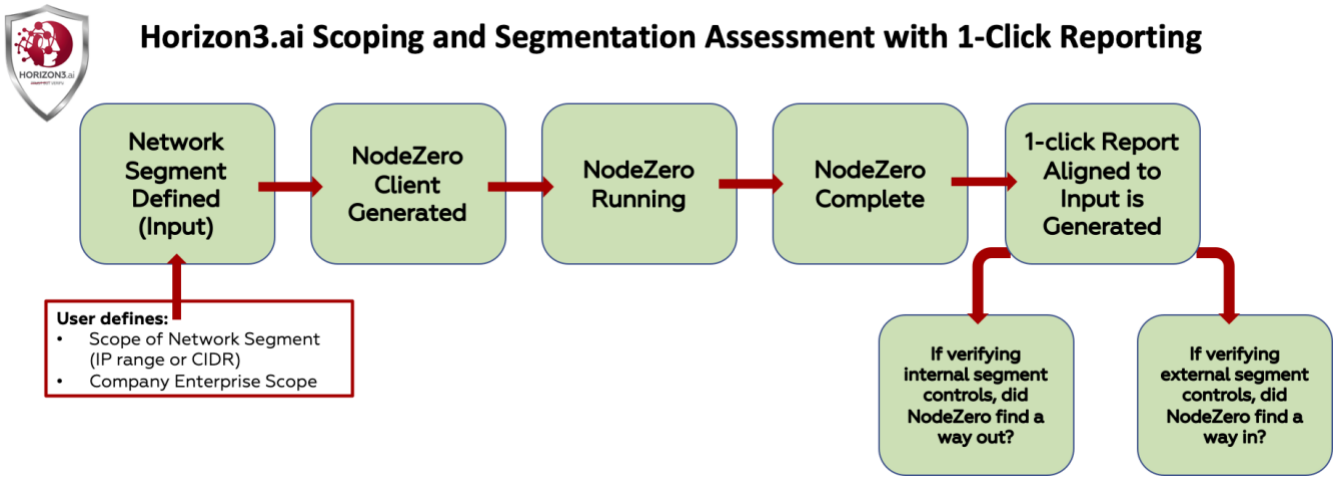
NodeZero can quickly and thoroughly assess your environment for PCI DSS compliance, SOC 2 security compliance and other compliance requirements. It can also be used for the required pentesting necessary to achieve compliance with these regulations.

Even better, NodeZero can take you beyond these requirements to help you ensure network security every day.

Scoping and Segmentation Assessment with 1-Click Reporting

NodeZero can verify if an attacker could pivot from one environment to another, by attacking from within or outside the defined segment, while also identifying any adjacent hosts that were "out of scope" but may have been reachable. **NodeZero** can be bound to a certain scope or unleashed to search, discover, and enumerate what it initially sees and then automatically expand scope based on what it has been able to benignly exploit.

NodeZero chains dangerous defaults, weak and default passwords (along with any for which it cracks hashes), exploitable vulnerabilities, as well as open ports, protocols and services, to verify if an attacker can move from one network segment into another.



Customer Profile: When preparing for their annual required PCI DSS pentest and audit, an online banking company pivoted from their traditional and expensive pentesting contract to **Horizon3.ai**. Within minutes, they launched a pentest operation spanning their entire enterprise. In only days, they were able to verify the CDE scope and security controls for their audit. All of this was achieved by utilizing **NodeZero**. With a single click, a comprehensive Scoping and Segmentation report generated in our portal provided the summary and details this regulation demands.

Although it is the foundation for creating a more secure environment for sensitive data and thereby reducing the scope of compliance audits, network segmentation can also be utilized to evolve to a zero-trust environment. The framework used to segment and scope your CDE or other sensitive data can be used for multiple network segments. The continuous, automated pen testing provided by **NodeZero**, along with a methodically segmented network, give you the building blocks you need to develop a true zero-trust environment.