Automated Pen Testing as a Service (APTaaS™)

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

Compliance In Security

Go from Compliant to Secure

Rules, Regulations, Laws = The Bare Minimum

There is no question, there are a plethora of best practices, frameworks, rules, regulations and laws that dictate, or even mandate, certain security standards:

- SOC/SOC 2/SOC 3 (financial reporting and service organization controls)
- PCI DSS (consumer transactions)
- GDPR/CCPA/CPRA (consumer privacy)
- HIPAA and the HITRUST Framework (healthcare)
- FERPA (education)
- NIST 800-171 (government sector)
- FFEIC and the Sarbanes-Oxley and Gramm-Leach-Bliley Acts (banking)
- and the list goes on and on…

It would take several of these papers to detail all of these, but the crux is basically the same – protect the data you need and properly purge it when you're done with it, especially the sensitive data you are stewarding for others.

However, compliance with standards does not mean security:

- Marriott was PCI DSS compliant when they were hacked.[1]

- SolarWinds was SOC 2 compliant when they, and hundreds of their customers, were hacked.[2]

- British Airways was fined for failing GDPR compliance…after they were hacked, and credit card data was stolen.[3]

"The year 2020 broke all records when it came to data lost in breaches and sheer numbers of cyber-attacks on companies, government, and individuals. In addition, the sophistication of threats increased from the application of emerging technologies such as machine learning, artificial intelligence, and 5G, and especially from greater tactical cooperation among hacker groups and state actors. The recent SolarWinds attack, among others, highlighted both the threat and sophistication of those realities."[4]

[1] https://www.pdcflow.com/payment-compliance/marriott-data-security-breach-lessons-why-pci-compliance-levels-matter/
[2] https://orangematter.solarwinds.com/2019/06/12/solarwinds-achieves-soc-2-type-ii-certification/#:~:text=We%20are%20pleased%20to%20announce,and%20by%20extension%2C%20their%20customers.
[3] https://www.natlawreview.com/article/british-airways-faces-significantly-reduced-20m-fine-gdpr
[4] https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/

It’s Time to Go from Compliant to Secure

Focusing on compliance with standards encourages a minimal assessment behavior, validating only once or twice per year or when there is a significant, purposeful change in the environment. The truth is that environments change constantly – employees come and go, software is updated, new systems are installed. Therefore, risks accrue every day, and your last compliance assessment becomes yesterday’s news.

The Federal Financial Institutions Examinations Council (FFEIC) defines Information Security as, “the process by which a financial institution protects the creation, collection, storage, use, transmission, and disposal of sensitive information, including the protection of hardware and infrastructure used to store and transmit such information.”[5]

Compliance with standards will not get your organization to this level of protection. You must go further.

True security is a continuously changing landscape — not a frozen snapshot in time. Achieving it requires constant vigilance, assessing and verifying your environment over and over, as often as every day. You need the tools and expertise on-hand to make this pattern of behavior a reality.

“It's not thinking of security as a state you can achieve, but it's a way of thinking of security as a process. And that's really something that helped us to address the different challenges in cybersecurity." – *Daniel Caduff, Deputy Head, ICT Division, Federal Office for National Economic Supply, Government of Switzerland, November 8, 2018*[6]

PCI DSS Compliance Applies to Nearly Everyone

Due to the ubiquitous use of online and onsite credit card payments, the Payment Card Industry Data Security Standard (PCI DSS) applies to organizations in nearly every industry.

PCI DSS compliance ensures that **all** entities — including merchants, processors, acquirers, issuers, and service providers – involved in payment card processing meet minimum levels of security when they store, process and transmit cardholder data (CHD). PCI DSS also applies to all other entities that store, process or transmit CHD and/or sensitive authentication data (SAD).[7]

At least once per year, if you accept credit card payments either online or onsite, or in any way touch cardholder data, you must comply with PCI DSS.

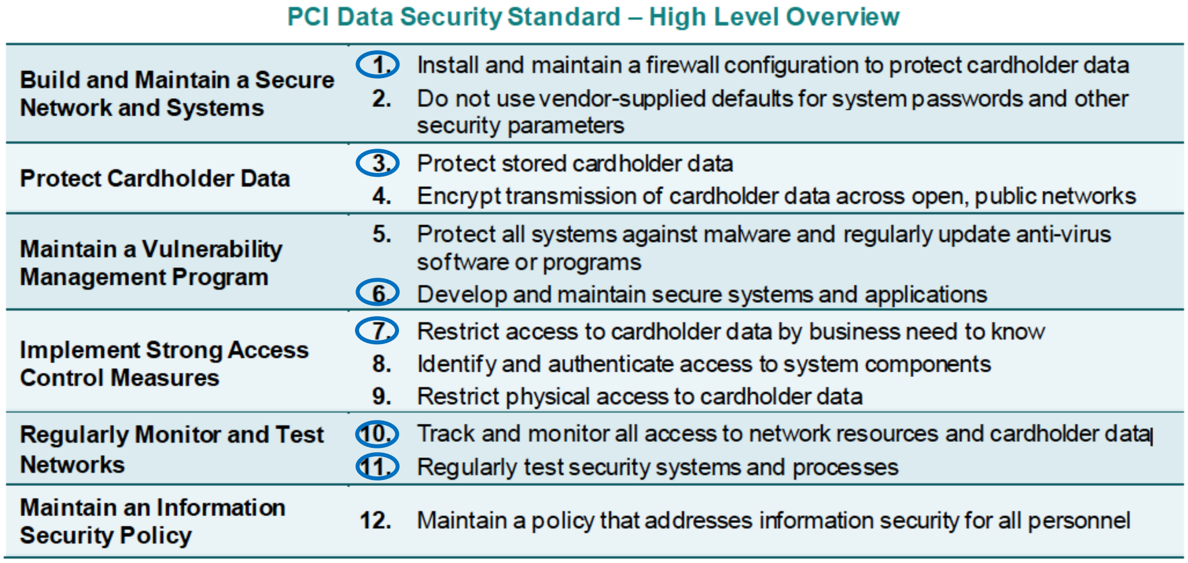
[5] FFIEC Information Technology Examination Handbook, Information Security, September 2016, https://www.ffiec.gov/cybersecurity.htm

[6] https://www.nist.gov/cyberframework/perspectives

[7] *Payment Card Industry (PCI) Data Security Standard*, v3.2.1

Network Segmentation is a Good Foundation for PCI DSS Compliance

Although it is not specifically required by PCI DSS, network segmentation helps you achieve many of its goals quickly and cost-effectively by isolating your cardholder data environment (CDE) and, therefore, reducing your PCI scope.



PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	○ 1.	Install and maintain a firewall configuration to protect cardholder data
	2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	○ 3.	Protect stored cardholder data
	4.	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5.	Protect all systems against malware and regularly update anti-virus software or programs
	○ 6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	○ 7.	Restrict access to cardholder data by business need to know
	8.	Identify and authenticate access to system components
	9.	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	○ 10.	Track and monitor all access to network resources and cardholder data
	○ 11.	Regularly test security systems and processes
Maintain an Information Security Policy	12.	Maintain a policy that addresses information security for all personnel

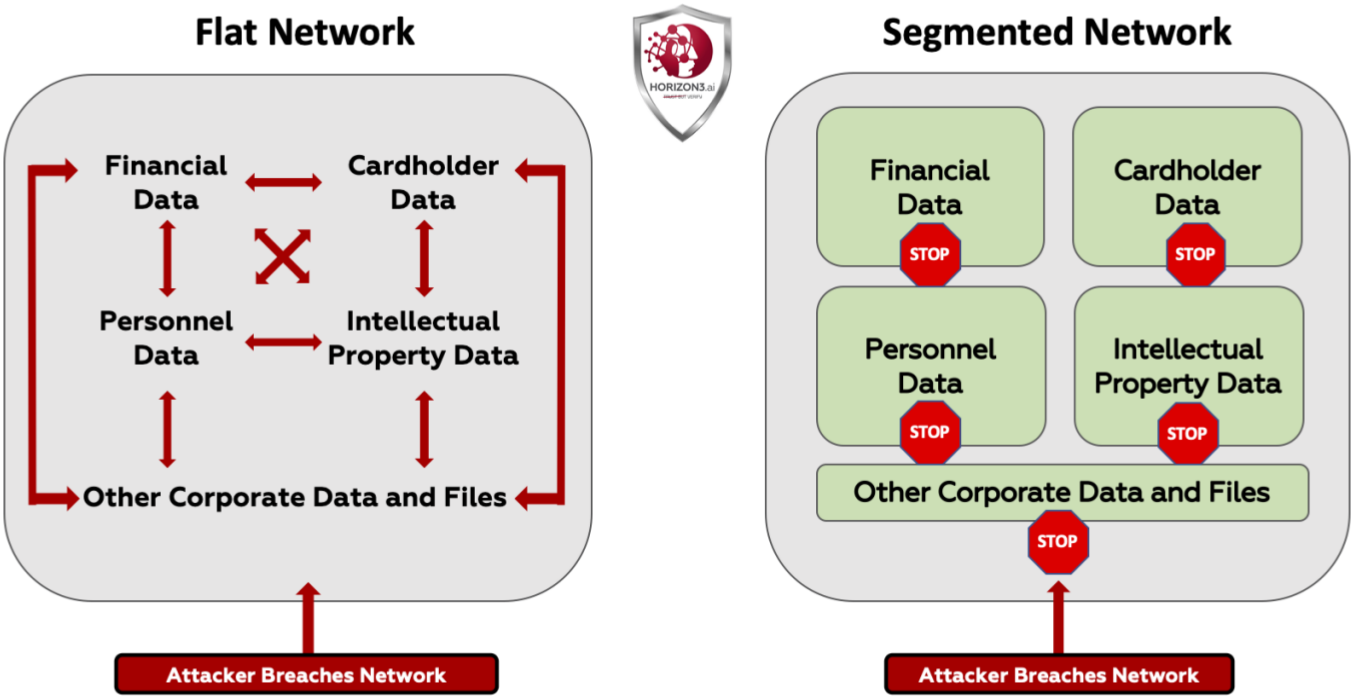
○ = related to network segmentation

"In addition to reducing risk, network segmentation can also reduce the time and cost associated with becoming PCI compliant. When organizations create a secure payment zone, separated from the rest of the day-to-day business traffic, they can better ensure their Cardholder Data Environment (CDE) only communicates with known and trusted sources. This limits the size of the CDE and potentially lowers your scope, which often reduces PCI requirements required for less-secure networks. Yes, segmentation is not necessarily required to be compliant with PCI DSS 3.2.1. **However, if you're looking for one of the easiest ways to reduce cost, effort, and time spent on getting in-scope systems compliant, you may want to consider segmentation.**"[7]

Additional 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.

"Network segmentation is a common practice where organizations reduce their risk within a network environment by isolating (segmenting) access to sensitive data between high-security networks (such as the Cardholder Data Environment) from less-secure networks (e.g., guest Wi-Fi). **When you use network segmentation, you can better ensure sensitive data is only sent to known and trusted users, devices, and/or sources.**"[8]


Flat Network
Financial Data
Cardholder Data
Personnel Data
Intellectual Property Data
Other Corporate Data and Files
Attacker Breaches Network
HORIZON3.ai
Segmented Network
Financial Data
STOP
Cardholder Data
STOP
Personnel Data
STOP
Intellectual Property Data
STOP
Other Corporate Data and Files
STOP
Attacker Breaches Network

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.

Node Zero can be used for the required pentesting for compliance with PCI DSS and also to assess the scope and segmentation of your CDE.

PCI DSS 3.2.1 requires that you, "develop and implement a methodology for penetration testing that includes external and internal penetration testing at least annually and after any significant upgrade or modification. If segmentation is used to reduce PCI DSS scope, perform penetration tests at least annually to verify the segmentation methods are operational and effective. Service providers using segmentation must confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after making changes to these controls."[7]

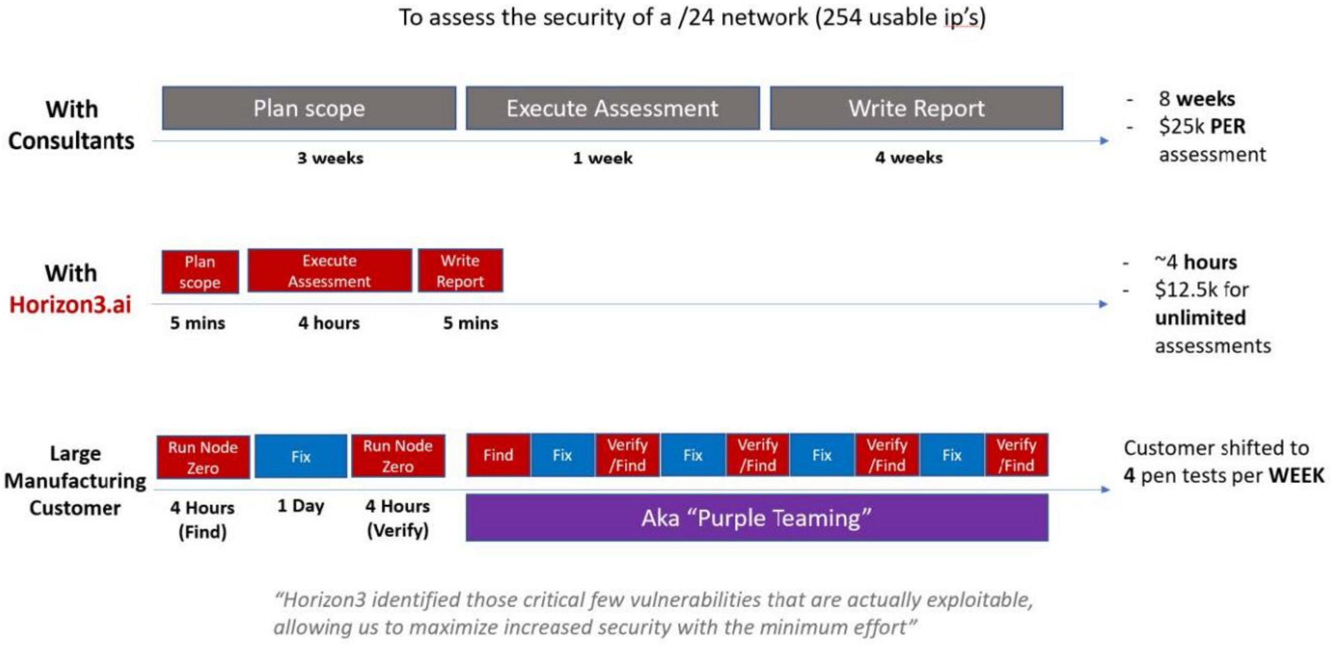
[8] https://www.securitymetrics.com/learn/how-to-perform-segmentation-checks

NodeZero can quickly and thoroughly assess your environment for PCI segmentation compliance, SOC 2 security compliance and other compliance requirements.

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

What Matters	**Traditional Approach**	**Better, Faster, Cheaper Approach**
Effort Required	High (Multi-Team, Coordinated)	Low (Self-Service, On Demand)
Test Frequency	Annual or Quarterly	Agile and Continuous
Total Cost	High for Single Pentest	Low for Unlimited Ops
Time to Value	Weeks to Written Report	Hours to Searchable Results
Coverage	1-2% of Environment	99+% of Environment
Expertise Needed	High to Execute	Low to Execute
Resources	External Professional Services	Internal Purple Team Partner
Ultimate Goal	**Pwn you to demonstrate value**	**Decrease risk to your company**

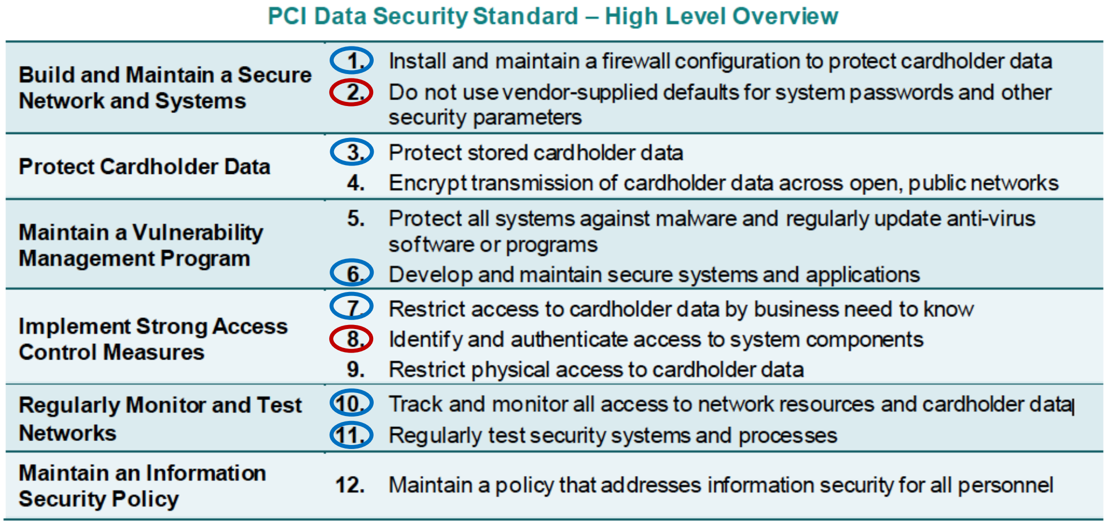
Unlike a laborious pen test that you may run once or twice a year, you can run NodeZero as often as you want. Horizon3.ai allows you to “turn the map around” and see your environment through the eyes of an attacker.


To assess the security of a /24 network (254 usable ip's)

“Horizon3 identified those critical few vulnerabilities that are actually exploitable, allowing us to maximize increased security with the minimum effort”

PCI DSS Scoping and Segmentation Compliance Assessment with 1-Click Reporting

Horizon 3 AI's PCI DSS Scoping and Segmentation Compliance Assessment utilizing NodeZero allows you to confirm your network segmentation, as part of your overall PCI DSS compliance posture—and as you move toward a zero-trust model.



PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	🔵 1. 🔴 2.	Install and maintain a firewall configuration to protect cardholder data Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	🔵 3. 4.	Protect stored cardholder data Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. 🔵 6.	Protect all systems against malware and regularly update anti-virus software or programs Develop and maintain secure systems and applications
Implement Strong Access Control Measures	🔵 7 🔴 8. 9.	Restrict access to cardholder data by business need to know Identify and authenticate access to system components Restrict physical access to cardholder data
Regularly Monitor and Test Networks	🔵 10. 🔵 11.	Track and monitor all access to network resources and cardholder data| Regularly test security systems and processes
Maintain an Information Security Policy	12.	Maintain a policy that addresses information security for all personnel

🔵 = network segmentation confirmed by NodeZero
🔴 = additional requirements assessed by NodeZero

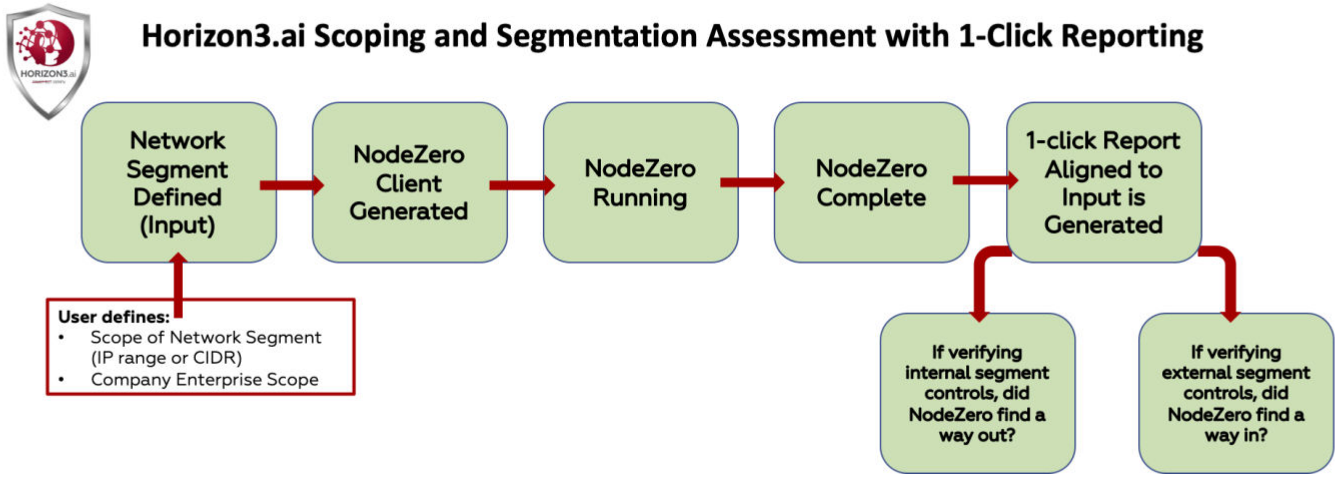
Scoping and Segmentation involves checking for two paths to the scope range:

1. is there an uncontrolled/undesired way in?
2. is there an uncontrolled/undesired way out?

NodeZero will 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 CDE 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.

And, when the pentest operation is complete, our portal provides you with a 1-click report you can use to support the scope of your PCI DSS compliance test.


Horizon3.ai Scoping and Segmentation Assessment with 1-Click Reporting

Network Segment Defined (Input)
NodeZero Client Generated
NodeZero Running
NodeZero Complete
1-click Report Aligned to Input is Generated
User defines:
• Scope of Network Segment (IP range or CIDR)
• Company Enterprise Scope
If verifying internal segment controls, did NodeZero find a way out?
If verifying external segment controls, did NodeZero find a way in?

Network Segmentation Isn't Only for Compliance

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.

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.