network perception

Solution
Overview

+1 (872) 245-4100

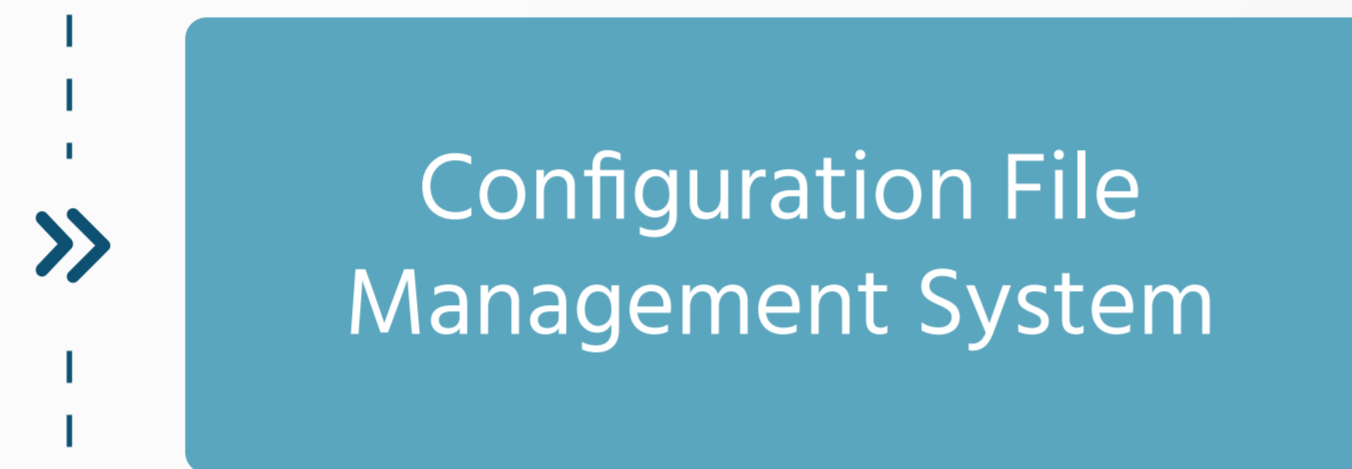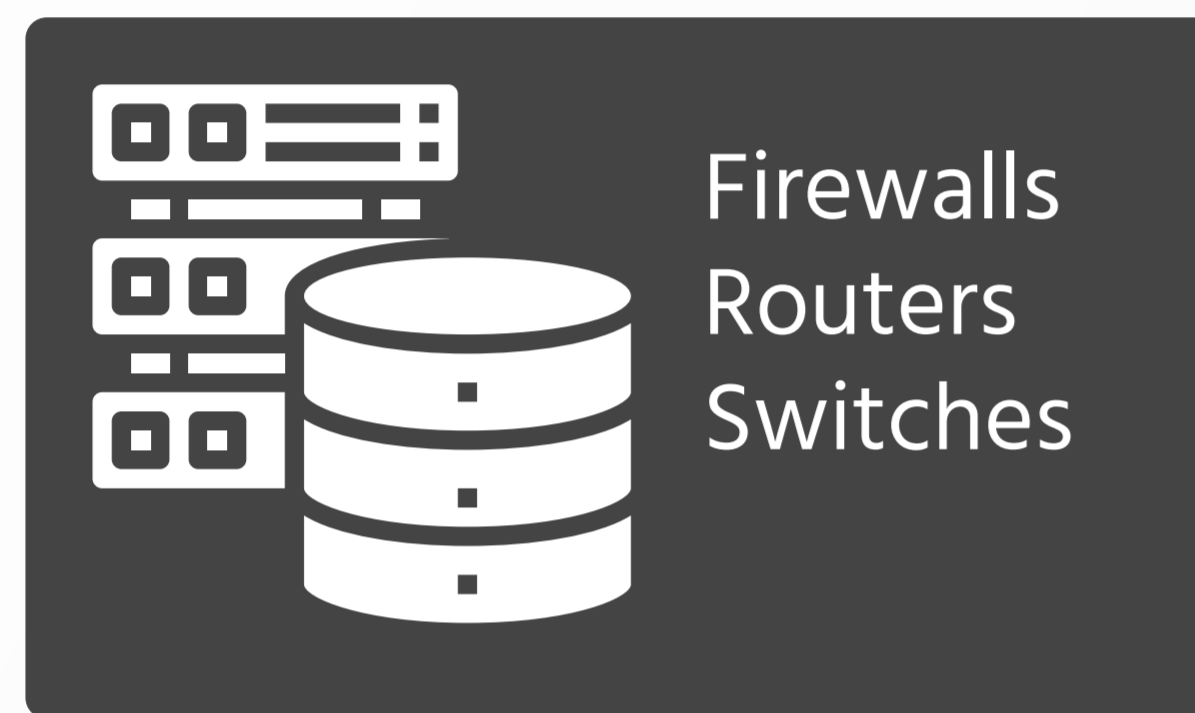info@network-perception.com

https://network-perception.com

Cybersecurity Demands-
The effect of this causes:

1 As device proliferation continues in OT environments, networks are under more strain

2 Cybersecurity has become paramount as adversaries target industrial control infrastructure

3 Regulators have shifted to Risk- Based Compliance

» These trends **increase demands** and the **costs** associated with maintaining compliance and security
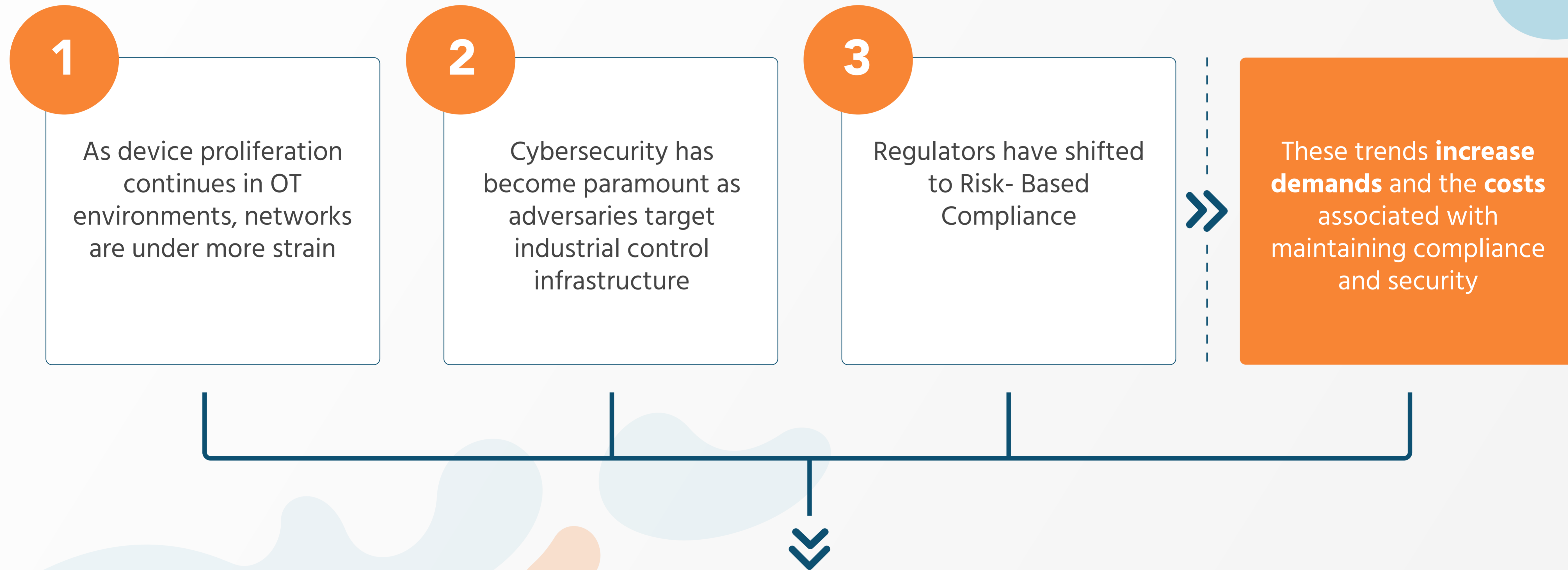
Cyber teams must manage additional risk without a proportional increase in resources

Solution: Independent Network Network Verification with NP-View™:

Firewalls Routers Switches

» **Configuration File Management System**

» **Network Access Modeling**

Access policy baseline

Rule justifications

Network diagrams

Network diagrams

✔ Founded from cybersecurity research at the University of Illinois

✔ Protecting 50% of top 30 largest power utilities in the US

Network Team

Security Team

Compliance Team

Auditors

Solving:

Risk of security drift

High expertise requirement

Speed to understanding

📞 +1 (872) 245-4100   ✉ info@network-perception.com   🌐 https://network-perception.com

NP network perception

About
Network Perception:

Our Mission is to Secure Critical Infrastructure

100+ customers /
50% of top 30
largest power
utilities in the US

Solved challenges
for **NERC** and
utilities through
ongoing
consultations

Leveraged in hundreds of
NERC CIP audits since 2016

Provide independent
visibility and proactive
protection

Founded by
**cybersecurity
experts** from the
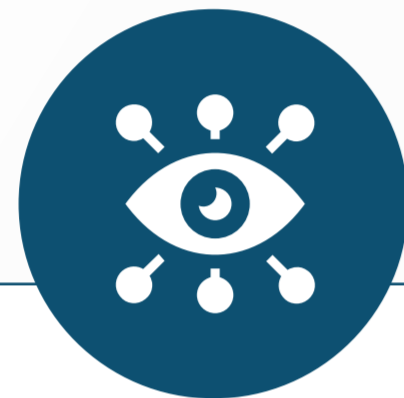University of Illinois
at
Urbana-Champaign

Research funded by
DOE, DHS, NSF

Network Perception:
Purpose-Built for OT Networks

Network Visualization & Mapping:
Continuously assess risks, enhance network segmentation, and prevent misconfigurations.

Proactive Security:
NP-View can continuously assess potential and active network changes and flag preventative alerts on policy conditions.

Lightweight & Effortless Setup:
NP-View provides a complete network view without the need to install an agent or write to the OT network.

Non-Invasive:
NP-View runs on-premise in an off-line mode and does not require an internet connection.

np network perception

Empower Cyber Teams
to meet increasing demands:

Reduce Immediate Costs

- Audit preparation
- Policy review
- Change validation
- Tech refresh / cyber hygiene

Mitigate Future Risk

- Network risk assessment
- Continuous configuration monitoring
- Proactive alerts

Improve Technology ROI

- Network traffic monitoring/asset discovery
- Vulnerability management
- Ticketing integration

Reduce
Immediate Costs:

Audit Preparation

Identify access rules that do not meet compliance requirements and create exposure

Policy Review

Ease the process of firewall configuration review and documentation

Change Validation

Automatically ensure any changes do not create overly permissive rules

Tech Refresh and Cyber Hygiene

Ensure hardware changes or replacements do not open network up to additional risks
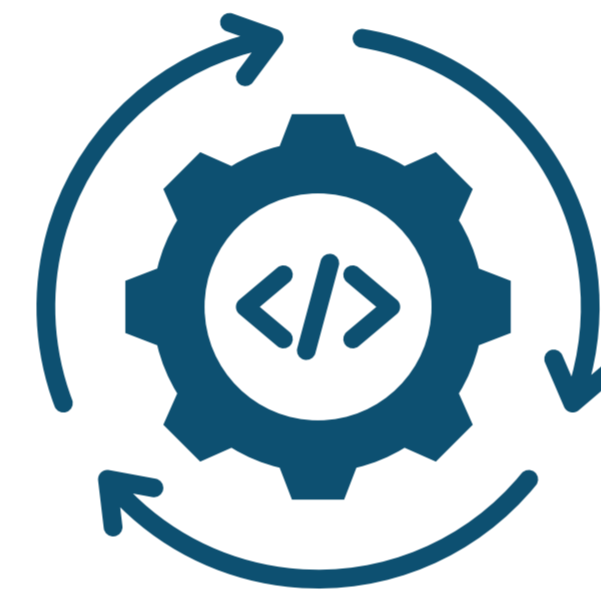
NP network perception

Mitigate Risks to
Eliminate Future Costs:

Network Risk Assessment

Measure overall risk of OT network and generate audit-grade reports to avoid additional resource allocation

Continuous Configuration Monitoring

Reduce security drift through automated change notifications and network change workflow
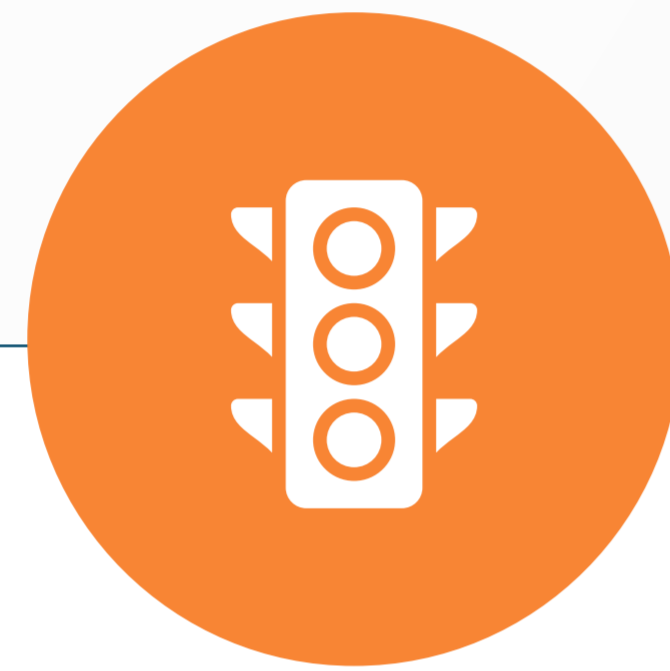
Proactive Alerting

Provide proactive alerts of overly-permissive rules to avoid future fines and reduce overall network risk

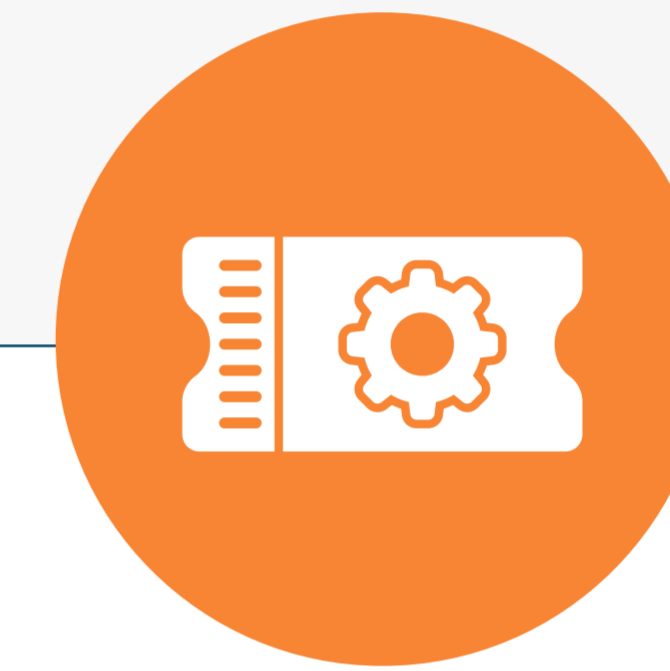# Enhance ROI from Existing Cyber Investments:

Network Traffic Monitoring / Asset Discovery
Enhance monitoring with asset context

Vulnerability Management
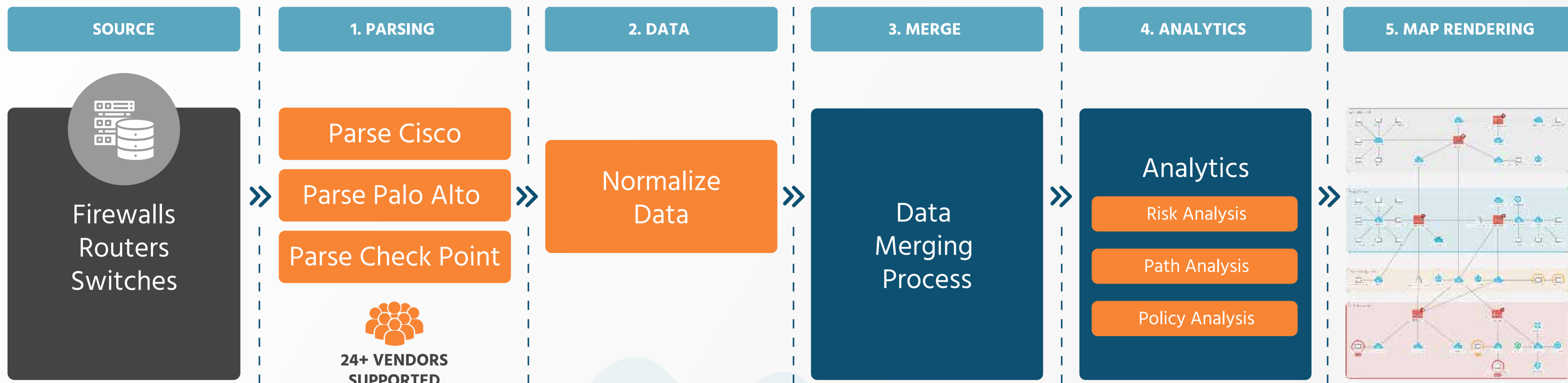**Prioritize** patching using NP Map and the ability of vulnerability to propagate

Ticketing Integration
Optimize OT network requests and change

NP network perception

NP-View: Read-only Pipeline Process:

SOURCE	1. PARSING	2. DATA	3. MERGE	4. ANALYTICS	5. MAP RENDERING

SOURCE

Firewalls
Routers
Switches

1. PARSING

Parse Cisco

Parse Palo Alto

Parse Check Point

24+ VENDORS SUPPORTED

2. DATA

Normalize Data

3. MERGE

Data Merging Process

4. ANALYTICS

Analytics

Risk Analysis

Path Analysis

Policy Analysis

5. MAP RENDERING

NP-View: Normalizing Raw Config & Auxiliary Data Into a Unified Network Topology
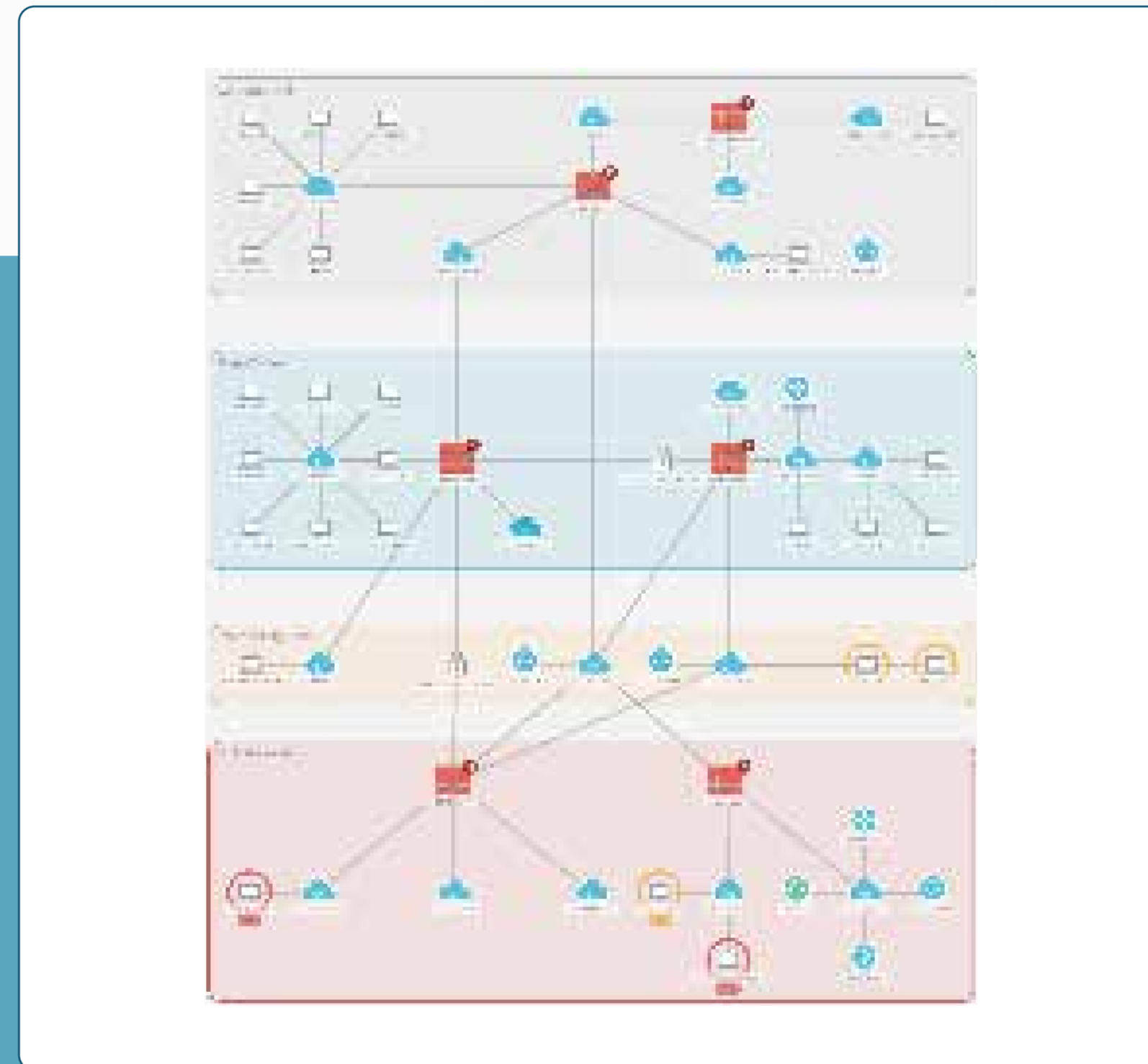• Proactive alerting of network changes with risk alerts   • Full network access path analysis

NP-View: Independent Network Access Modeling & Verification:

Firewalls
Routers
Switches

Network architecture

Access path modeling

Zones & criticality

Asset metadata / annotation

ℹ **NP-View Read-only Network Access Modeling Platform:** 1 Code Base, 2 On-prem Packages

NP-View Desktop
- Single-user
- Manual Configuration Ingestion
- Point-in-time Network Analysis & Modeling

NP-View Server
- Multi-user
- Automated Configuration Ingestion
- Automated Alerts & Notifications

📞 +1 (872) 245-4100   ✉ info@network-perception.com   🌐 https://network-perception.com

Zone Matrix

WHAT is Zone-to-Zone?

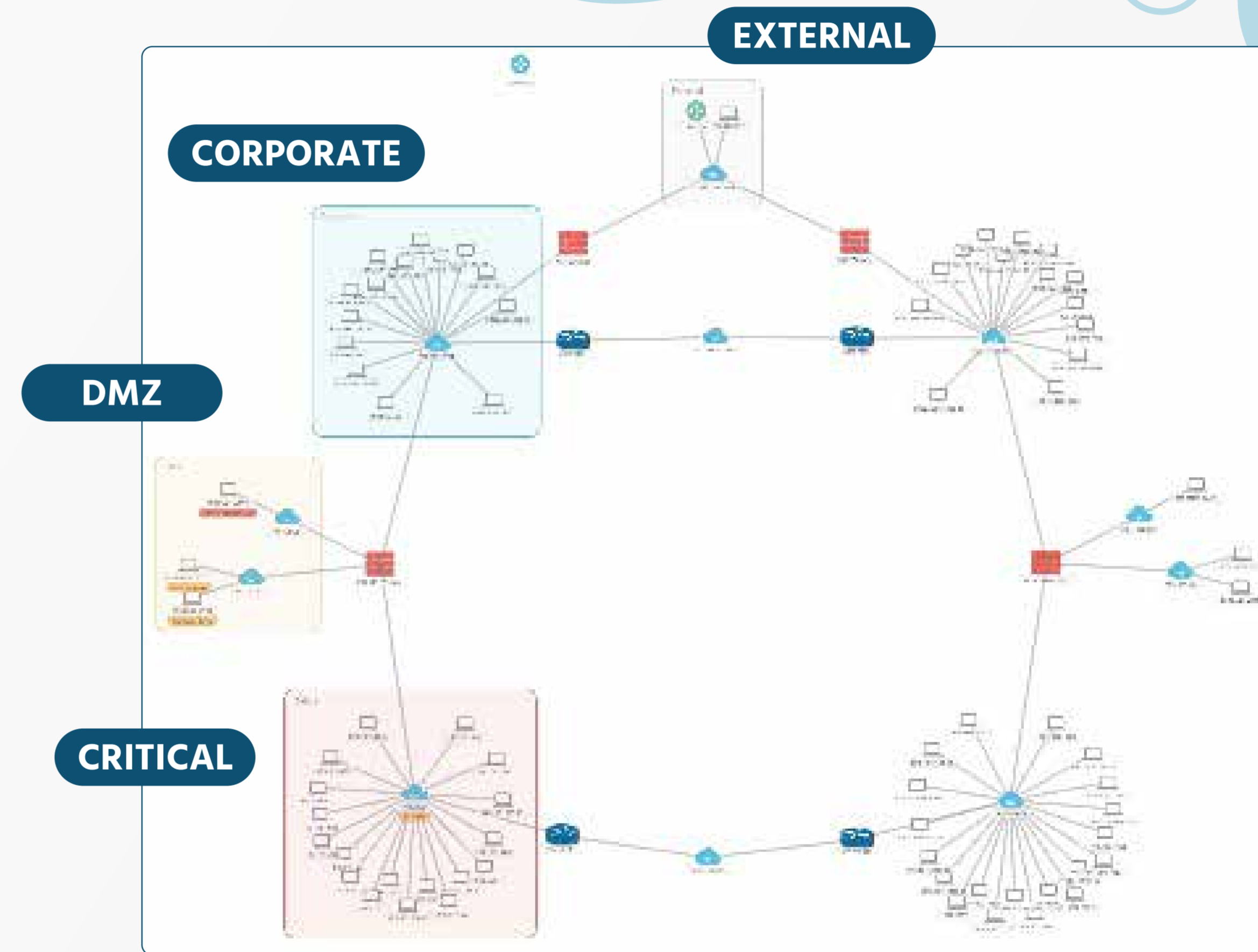**Shows permitted** network segmentation instantly

WHY it's important?

Complex networks make access assessment difficult

HOW will it enable?

Segmentation matrix provides key zone-to-zone access insights

EXTERNAL

CORPORATE

DMZ

CRITICAL

Segmentation Matrix

From/To	Corporate	Critical	DMZ	External
Corporate		TCP/443 TCP/3389	TCP/443	TCP/443 TCP/8531
Critical	Denied		Denied	TCP/443 TCP/53 TCP/8531
DMZ	TCP/443	Denied		TCP/443
External	TCP/3389 TCP/8531	Denied	TCP/3831	

Investing in
Strategic Partnerships:

Partner Ecosystem: Better Together

DEVICE MANUFACTURERS

Ingest device configurations seamlessly

Alcatel·Lucent NOKIA · aws · Azure · Check Point SOFTWARE TECHNOLOGIES LTD. · CISCO

DELL · enterasys Secure Networks · FORTINET · HIRSCHMANN A BELDEN BRAND · aruba a Hewlett Packard Enterprise company

extreme networks

JUNIPER NETWORKS · IPTABLES · NETGEAR · paloalto NETWORKS · pfsense

RUGGEDCOM · SIEMENS · SEL SCHWEITZER ENGINEERING LABORATORIES · SONICWALL · SOPHOS

OPERATIONAL VENDORS

Close the loop on operational use cases

servicenow

splunk>

SECURITY VENDORS

Greater insights with NP topology intelligence

CLAROTY · GRAYMATTER

OPSCURA · txOne networks

CONSULTING FIRMS

Eliminate human errors and accelerate analysis

Deloitte. · ABS Group

westMONROE · ARMEXA

AMPERE

NP network perception

Hear from our Customers:

"We do a lot of assessments. NP View has allowed us to **streamline our process** and **save our clients time and money.**"

-INDUSTRIAL CONTROLS ENGINEERING FIRM

"Prior to NP-View, it would take 2 engineers 16 hours to **analyze a single firewall**. Now, we complete a more comprehensive view **in only two hours!**"

-GLOBAL CONSULTING FIRM

"Manually, it would take 1 month of effort to **complete a site review**, but NP-View allows us to collapse that down to **2-4 hours!**"

-GLOBAL O&G CLIENT

"NP-View provides a **standardized approach** to validating the state of network assets & configurations."

-EXTERNAL AUDITOR

Contact Us:

There were
6000 vulnerabilities
in 2016 and
18,000 vulnerabilities
in 2022.

About Network Perception & NP-View

Network Perception protects industrial control systems by ensuring network access security as the first line of perimeter defense. NP-View software provides complete network transparency and continuous mapping to better support cybersecurity compliance and enable greater cyber resiliency.

Launched in 2014 at the University of Illinois at Urbana-Champaign Research Park, Network Perception was founded by a team of experts on network security and critical infrastructure protection and is inspired and informed by ongoing consultations with NERC, FERC, DOE, and DHS.

📞 **+1 (872) 245-4100**

✉ **sales@network-perception.com**

🌐 **https://network-perception.com**

💡 **https://kb.network-perception.com**

Request a Demo

network perception

Two Sides
of Visibility:

Network Perception provides a unique and lightweight **network access modeling** technology that complements traditional network traffic monitoring to offer a comprehensive network visibility solution.
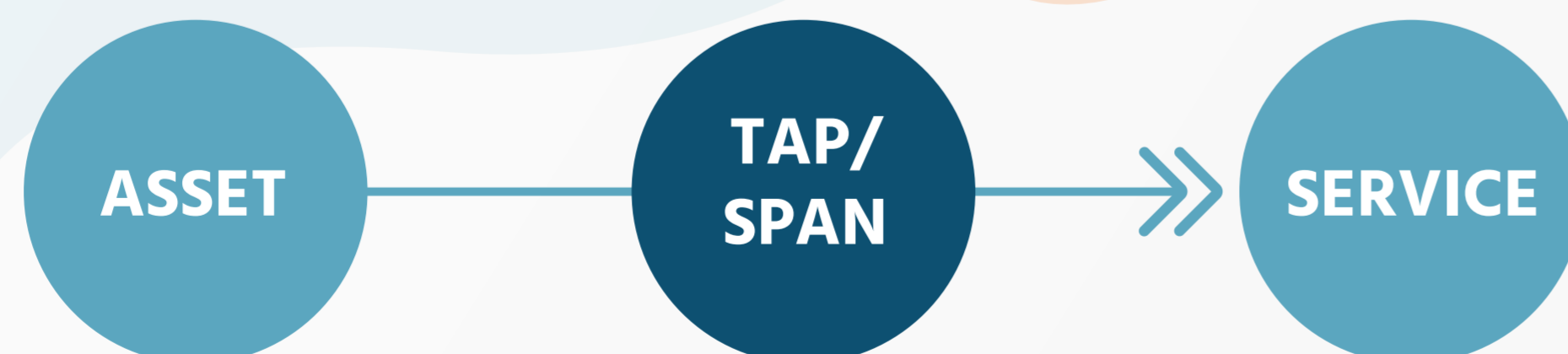
Analytic Monitoring:
Monitor and detect adverse actions and conditions in a timely and actionable manner.

Which assets are connecting to which services

Network Traffic Monitoring

ASSET — TAP/SPAN »» SERVICE

REQUIRES NETWORK INSTRUMENTATION WITH SENSORS

Dynamic Representation:
Keep the representation of the network current. Enhance understanding of dependencies

Which assets can connect to which services

Network Access Modeling

ASSET - - - FIREWALL - - - »» SERVICE

NO SENSOR APPROACH: ONLY FIREWALL CONFIG NEEDED

+1 (872) 245-4100   info@network-perception.com   https://network-perception.com