

# Foundational network configuration security

Zero Trust and PCI DSS v4.0  
assurance at scale





# Agenda

## PCI DSS and Zero Trust

- Protecting the CDE... and beyond
- PCI DSS v4.0 – leading the way
  1. Effective network segmentation
  2. Risk Assessments
  3. Avoid sampling where automation allows
  4. Security as a continuous process
- Nipper Enterprise Demo
  1. Continuous Auditing
  2. Proactive Auditing

**“Firewalls can’t solve today’s most urgent security priorities. After all, more than 80 percent of network traffic is inside the perimeter.”**

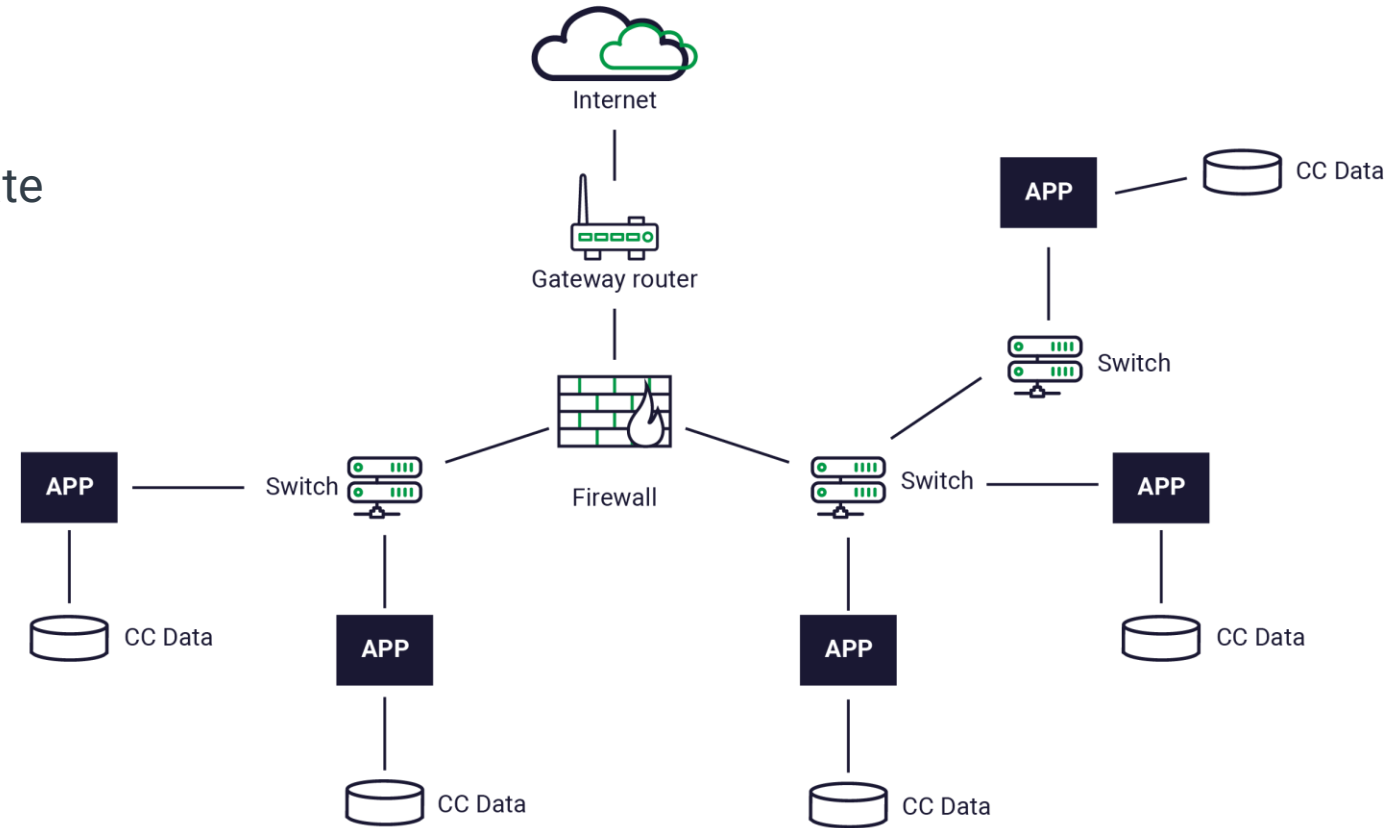
**Guardicore Centra / Forrester**



# Protecting the CDE and beyond...

## Best Practices in Network Segmentation

- ✓ Minimises attack surface of critical real estate
- ✓ Reduces susceptibility to ransomware
- ✓ Prevents lateral movement across the network
- ✓ Allows for the assessment of each and every device, rather than a sample
- ✓ Improves ability to consistently meet compliance
- ✓ Foundational component of Zero Trust network access



[US Depart of Defense Zero Trust Reference Architecture](#)



# PCI DSS v4.0 – Leading the way

Major change in standards to deliver security from compliance

## PCI DSS v4.0

1. Meet the security needs payment industry
2. Promote security as continuous process
3. Add flexibility for different methodologies
4. Enhance validation methods

### Zero Trust Best Practices:

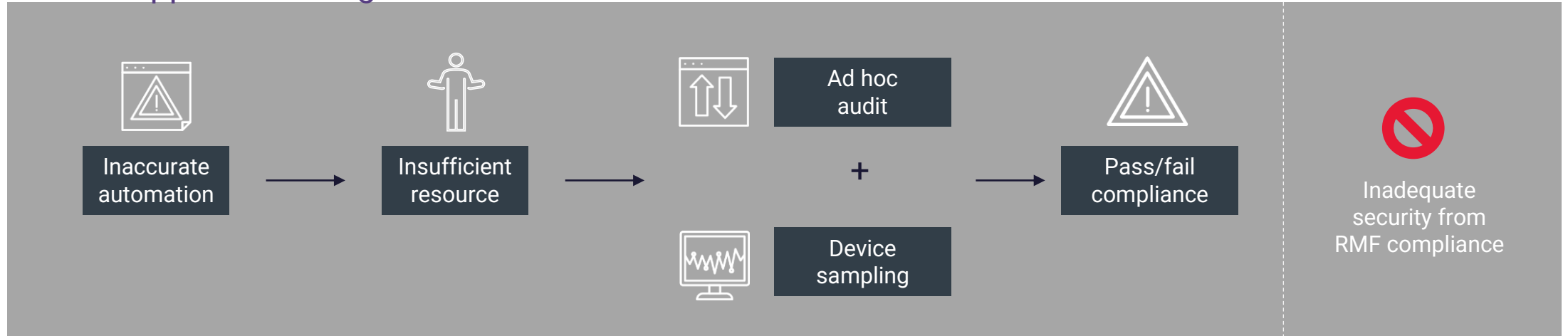
- ✓ Effective network segmentation
- ✓ Risk assessments inform policy enforcement cadence
- ✓ Leverage automation to automate auditing of every device/asset
- ✓ Risk prioritized mitigation



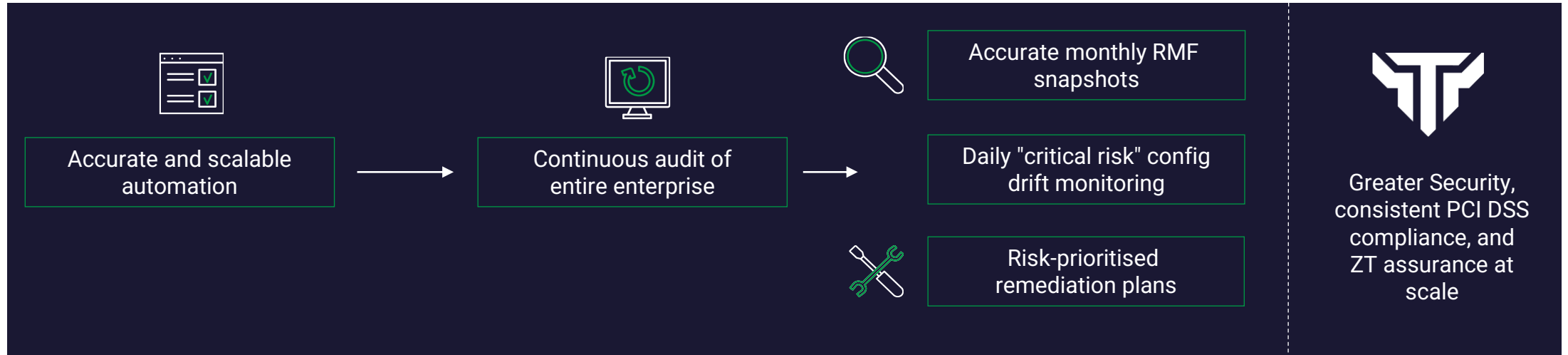
# Security as a Continuous Process

Configuration Drift

Current approach failing:



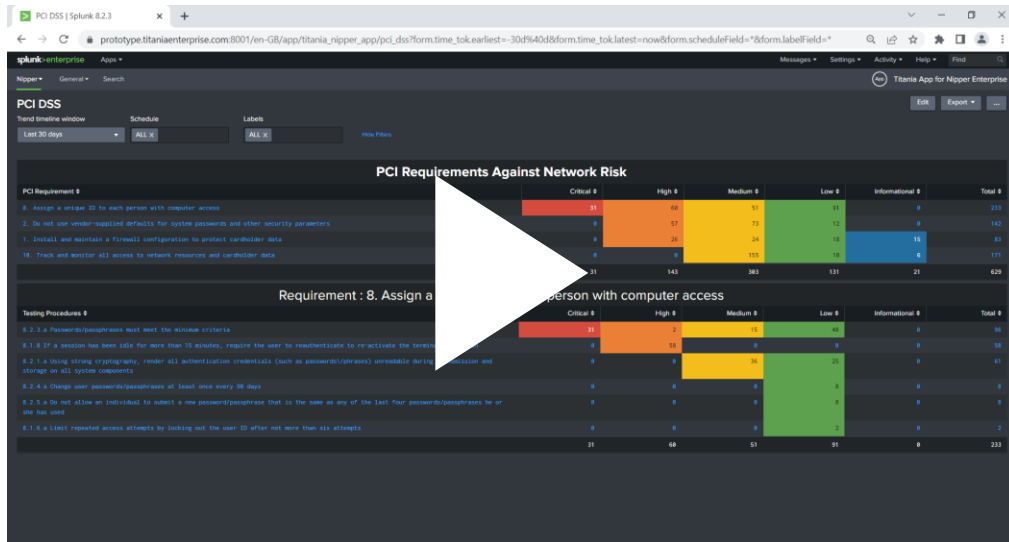
Best practice continuous approach required:



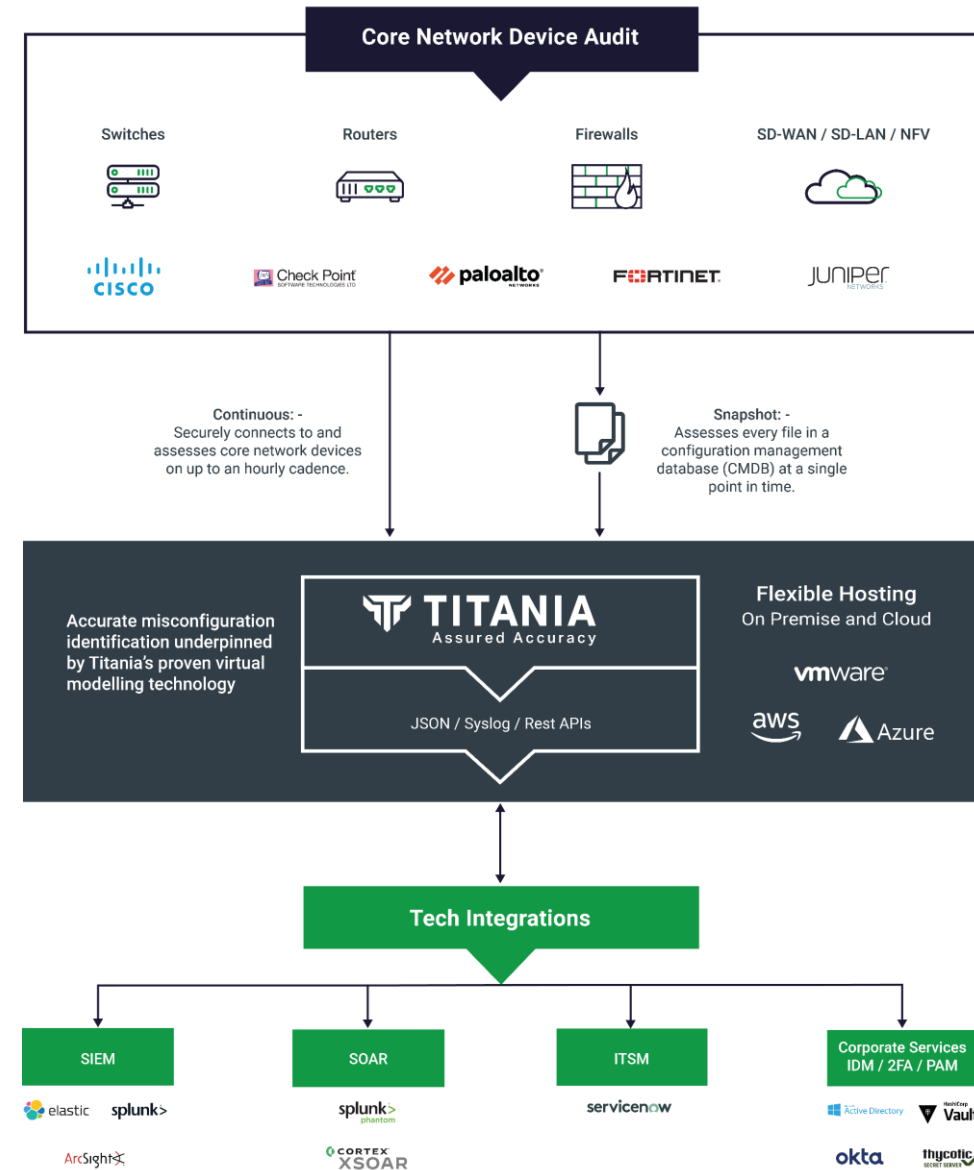


# Nipper Enterprise Demo

## Accurate PCI DSS compliance posture assessments



## NIPPER ENTERPRISE: TECHNOLOGY & DEVICE INTEGRATIONS





## Any questions?

**“Human error creates the biggest threat. Technicians can inadvertently misconfigure devices, opening holes. So, we need to go back and validate configs.”**

Steve Wallace | DISA Emerging Technology Directorate

**“Without evidence from assurance processes, it’s very difficult to make credible risk-based decisions.”**

Dr. Ron Ross | NIST Systems Security Engineering Project Lead

## Visit us:

Stand A12

[Titania.com](http://Titania.com)

## Thank You.

Ian Robinson | Chief Architect

[Ian.Robinson@titania.com](mailto:Ian.Robinson@titania.com)



Titania, Security House, Barbourne Road, Worcester, WR1 1RS.



Titania, Suite 600, 2451 Crystal Dr, 6<sup>th</sup> Floor. Arlington. VA. 22202.