NIPPER
ENTERPRISE

Titania

Continuous, Enterprise-wide Zero Trust and CORA Attack Surface Management Assurance

March 2024

Titania: U.S. Critical National Infrastructure (CNI) Overview

10+ years supporting DoD and US CNI cybersecurity requirements for firewalls, routers and switches

Nipper trusted by 30+ USG agencies, including:

- DoD, IC, DHS (TSA), DoE and National Guard

Nipper used in AF CVA/H weapon system since 2013

- CPTs, Air National Guard – Vulnerability and DISA STIG assessments

Nipper automation accuracy scaled for the enterprise

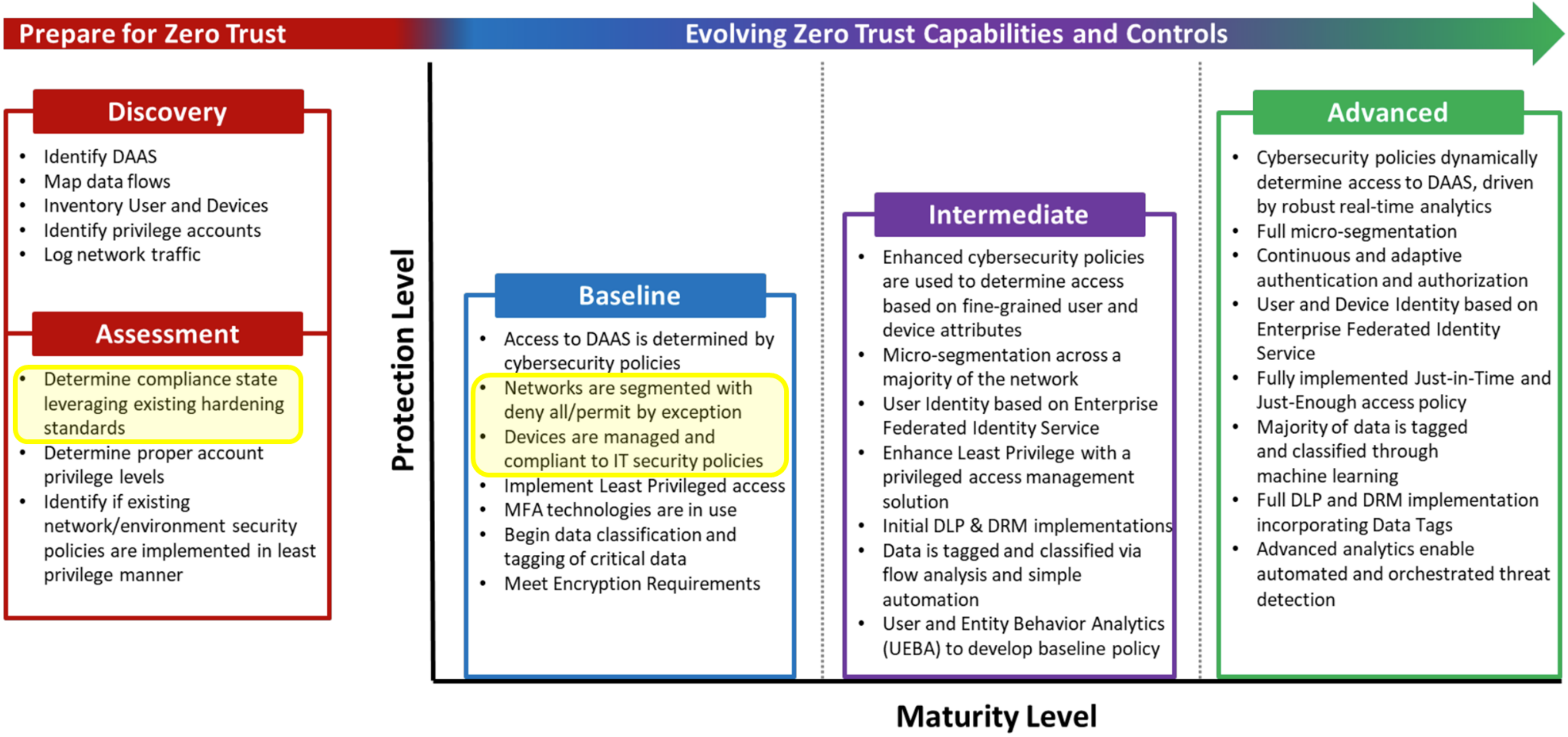
- Secure webapp assesses up to 250,000 firewalls, routers and switches per day. On-demand for CPTs or continuously for NOC and SOC teams

Enterprise-wide mission readiness and resilience assurance

- DOD Comply to Connect (C2C), Zero Trust (ZT) and Cyber Operational Readiness Assessment (CORA) attack surface visibility

Enterprise-wide ZT Policy and Segmentation Assurance

Source: U.S. Department of Defense Zero Trust Reference Architecture



Prepare for Zero Trust

Evolving Zero Trust Capabilities and Controls

Discovery

- Identify DAAS
- Map data flows
- Inventory User and Devices
- Identify privilege accounts
- Log network traffic

Assessment

- Determine compliance state leveraging existing hardening standards
- Determine proper account privilege levels
- Identify if existing network/environment security policies are implemented in least privilege manner

Baseline

- Access to DAAS is determined by cybersecurity policies
- Networks are segmented with deny all/permit by exception
- Devices are managed and compliant to IT security policies
- Implement Least Privileged access
- MFA technologies are in use
- Begin data classification and tagging of critical data
- Meet Encryption Requirements

Intermediate

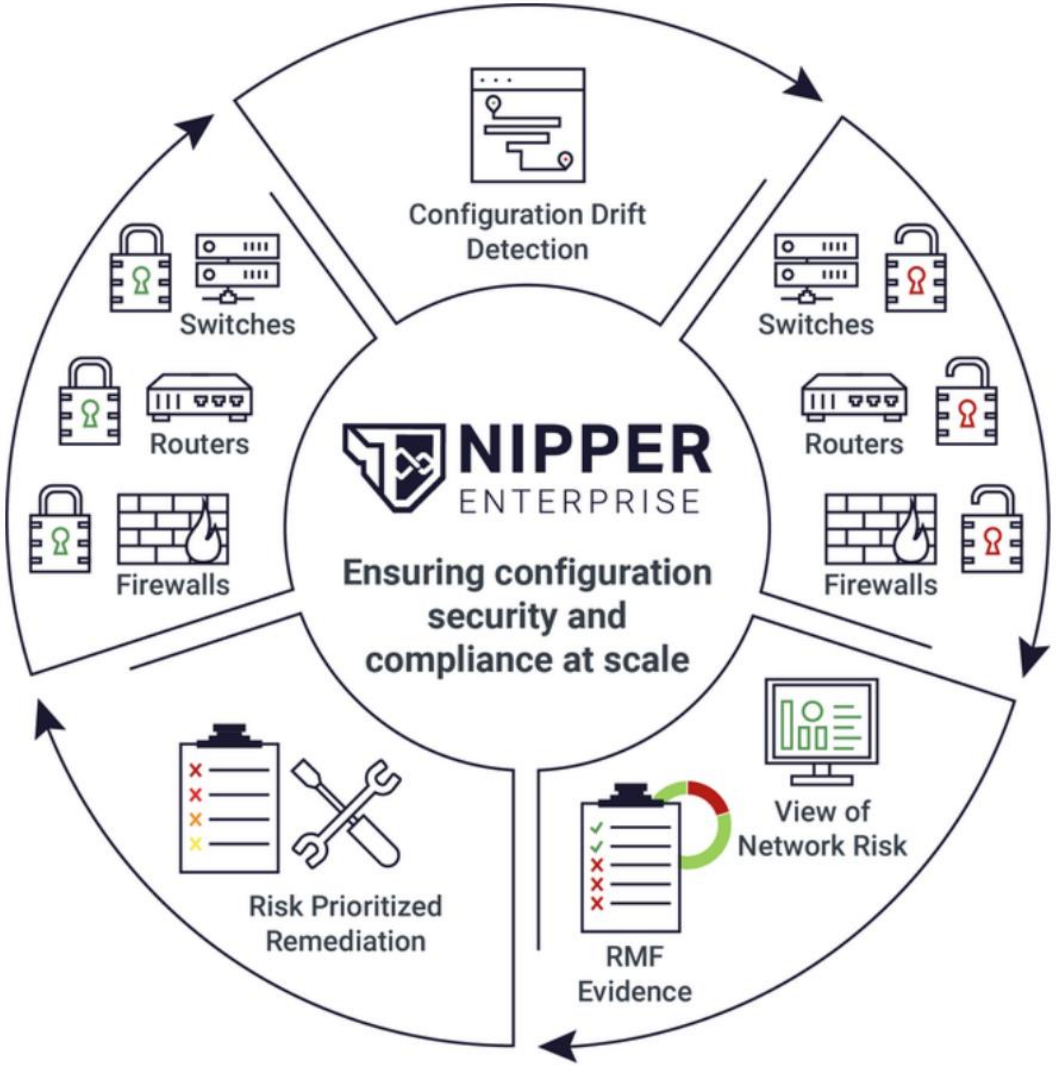
- Enhanced cybersecurity policies are used to determine access based on fine-grained user and device attributes
- Micro-segmentation across a majority of the network
- User Identity based on Enterprise Federated Identity Service
- Enhance Least Privilege with a privileged access management solution
- Initial DLP & DRM implementations
- Data is tagged and classified via flow analysis and simple automation
- User and Entity Behavior Analytics (UEBA) to develop baseline policy

Advanced

- Cybersecurity policies dynamically determine access to DAAS, driven by robust real-time analytics
- Full micro-segmentation
- Continuous and adaptive authentication and authorization
- User and Device Identity based on Enterprise Federated Identity Service
- Fully implemented Just-in-Time and Just-Enough access policy
- Majority of data is tagged and classified through machine learning
- Full DLP and DRM implementation incorporating Data Tags
- Advanced analytics enable automated and orchestrated threat detection

Mission Assurance on the Network for Firewalls, Routers and Switches

Risk-prioritized remediation delivers enterprise-wide readiness and resilience assurance from:



Configuration Drift Detection
Switches
Routers
Firewalls
Switches
Routers
Firewalls
NIPPER ENTERPRISE
Ensuring configuration security and compliance at scale
View of Network Risk
RMF Evidence
Risk Prioritized Remediation

1. On-demand CPT or continuous SOC visibility of:

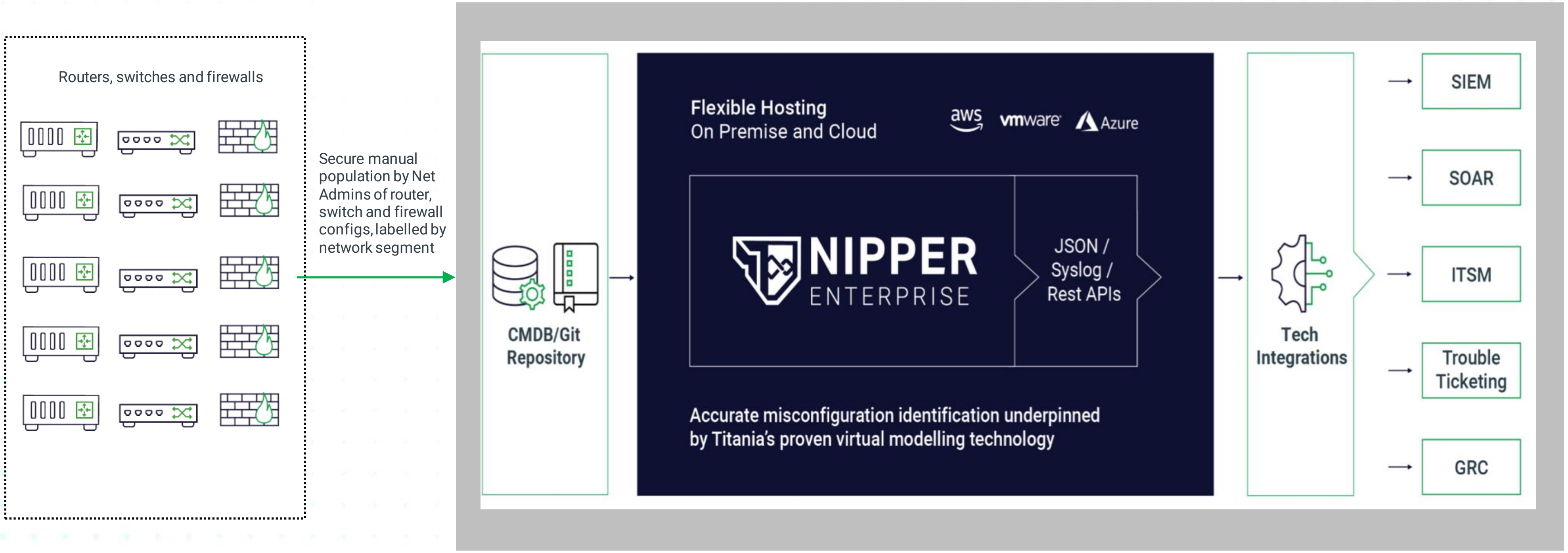
- ZT policy enforcement and segmentation posture
  - ✓ DISA STIG & CISA KEV enforcement posture
  - ✓ Segmentation blacklists – IPs, ports, accounts
- CORA attack surface posture and forensics
  - ✓ STIGs and KEVs mapped to MITRE ATT&CK
  - ✓ Historic ATT&CK forensics for threat hunters
- Attack vector exposure by network segment
  - ✓ Privilege escalation and lateral movement exposure
  - ✓ TTP reporting for specific APTs and ransomware
- Mandated RMF compliance – pass/fail device reports

2. Continuous NOC visibility of every network change

3. Continuously updated and segmented CMDB

2 Steps to Continuous Enterprise-wide ZT and CORA ASM Assurance

Step 1 - On-demand enterprise-wide / base-wide mission readiness and resilience visibility



Routers, switches and firewalls

Secure manual population by Net Admins of router, switch and firewall configs, labelled by network segment

CMDB/Git Repository

Flexible Hosting
On Premise and Cloud

aws vmware Azure

NIPPER ENTERPRISE

JSON / Syslog / Rest APIs

Accurate misconfiguration identification underpinned by Titania's proven virtual modelling technology

Tech Integrations

SIEM

SOAR

ITSM

Trouble Ticketing

GRC

git

servicenow

elastic

splunk>

DISA

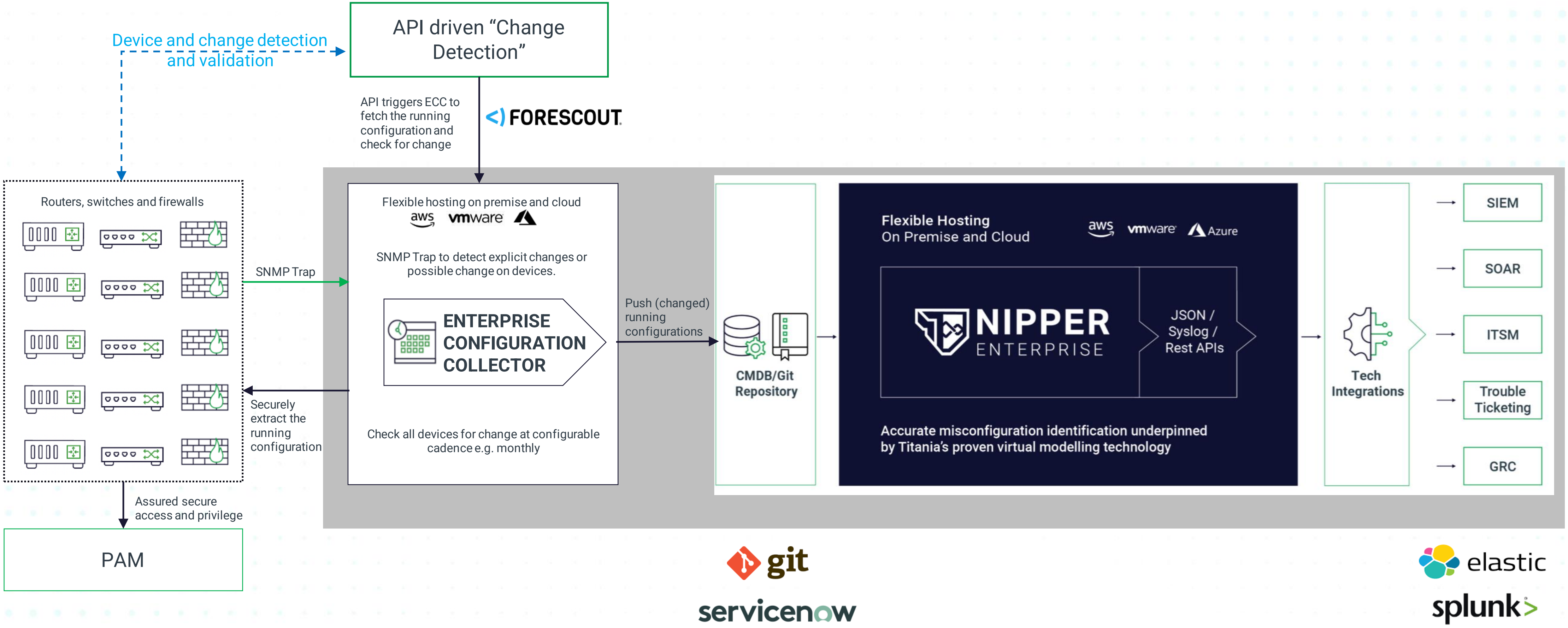
MITRE | ATT&CK®

NIST

Goal: Automate on-demand CORA posture visibility at the start and end of base assessments, allowing CPTs to focus on attack surface reduction through operational risk-prioritized vulnerability remediation and threat hunting

2 Steps to Continuous Enterprise-wide ZT and CORA ASM Assurance

Step 2 – Continuous, proactive enterprise-wide mission readiness and resilience assurance



Device and change detection and validation
API driven "Change Detection"
API triggers ECC to fetch the running configuration and check for change
FORESCOUT
Routers, switches and firewalls
SNMP Trap
Flexible hosting on premise and cloud
aws
vmware
SNMP Trap to detect explicit changes or possible change on devices.
ENTERPRISE CONFIGURATION COLLECTOR
Securely extract the running configuration
Check all devices for change at configurable cadence e.g. monthly
Push (changed) running configurations
CMDB/Git Repository
Flexible Hosting On Premise and Cloud
aws
vmware
Azure
NIPPER ENTERPRISE
JSON / Syslog / Rest APIs
Accurate misconfiguration identification underpinned by Titania's proven virtual modelling technology
Tech Integrations
SIEM
SOAR
ITSM
Trouble Ticketing
GRC
Assured secure access and privilege
PAM
git
servicenow
elastic
splunk>

Goal: Automate continuous and holistic enterprise-wide ZT and CORA attack surface visibility and operational risk-prioritized remediation, assuring mission readiness and resilience on the network

Titania contacts

Phil Lewis – SVP of Enterprise Business Development, phil.lewis@titania.com

Ian Robinson – Chief Architect, ian.robinson@titania.com

Matt Malarkey – VP Strategic Alliances, matt.malarkey@titania.com