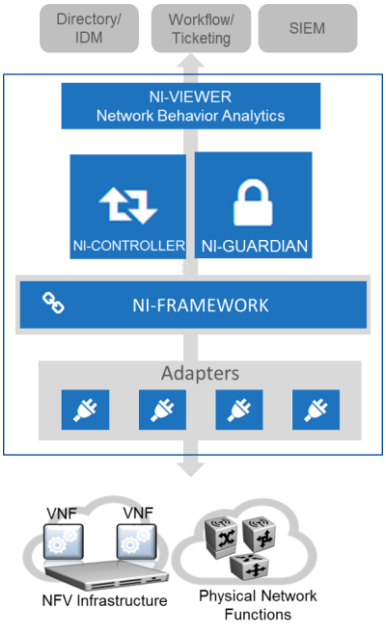
NI-DEFENDER Secure Network Auditing Platform

A new class of network security solution for todays and tomorrow's NFV, SDN and Cloud Networks

NI-DEFENDER is a Secure Network Auditing Platform (SNAP). It combines advanced network protection, network policy threat detection, and big data threat analytics. NI-DEFENDER is part of a holistic security and network integrity assurance strategy, providing a service-driven and contextual view of security access control policies. It is the industry's only solution addressing complex, heterogeneous, and demanding needs of communication service providers. It provides privileged user identity access management and control with correlated insight, blending network access and configuration state analytics for network anomaly detection.

Solution Overview

NI-DEFENDER integrates Nakina's best-in-class network integrity applications NI-GUARDIAN and NI-CONTROLLER, and overlays NI-VIEWER for data visualization.



NI-VIEWER is new Network Behavior Analytics layer to correlate network configuration and security data, providing real time, service-aware, contextual, data visualization and reporting.

NI-GUARDIAN secures and protects physical and virtual network functions and resources with a unified identity access management strategy, providing network-wide attribute and role-based identity access policy management and single-sign for users and operations systems.

NI-CONTROLLER is a network configuration data auditing application. It delivers detailed analytics outlining mismatched network and service configuration parameters, alerting network operators and pin-pointing network security vulnerabilities and anomalies.

Prevent, Pin-Point, Neutralize network security threats

Identity Access Management, Continuous Network Configuration Scanning, Advanced Analytics

Enable SecOps and NetOps to keep pace with DevOps

Defend today's networks, NFV and SDN

As the components are built on NI-FRAMEWORK, Nakina's Orchestration Enablement platform, NI-DEFENDER provides unparalleled scalability to millions of network elements and functions, supporting tens-of-thousands of simultaneous user accesses, and spans multi-vendor, heterogeneous, mobile, wireline, and cloud networks. All of NI-DEFENDER building blocks can be virtualized and are Cloud-ready.

Eliminate Security by Obscurity

SNAP addresses the growing security needs of service providers to protect today's and tomorrow's networks. The rapid evolution towards NFV and SDN poses significant security challenges and risks. Virtualization introduces multi-tenancy with the need to establish flexible attributed and role-based access control policies for both humans and autonomous systems.

NFV also introduces multiple layers of interdependencies (e.g. MANO, VNFs, NFVI, physical network functions), which will drive more complex policies. Domain isolation between these different slices will be needed, along with flexibility to create access management rules as needed. Network implementations, services, and operations practices will vary by operator, by service, by region so access management solutions must be adaptable and flexible.

Network behavior analysis is an integral part of next generation security strategies. Autonomous management and orchestration processes results in more dynamic and fluid networks. Virtual network infrastructure configuration changes are more frequent, virtual network functions are being instantiated, retired, changed, and moved. The automated systems and humans accessing network resources to activate, change, monitor and troubleshoot services are growing. It is be vital to correlate network configuration and service parameter changes with security events. This is absolutely crucial to pin-point configuration changes which may create security risks and to rapidly identify network access resulting in malicious attacks.

New, programmable, agile approaches to networking is creating a new type of paradigm within the industry – DevOps. As such as new type or network protection and security strategy is needed. NI-DEFENDER sits at the nexus of SecOps and NetOps. SNAP unifies the rich data from security and network operations providing service providers the right service-aware insight in order to pin-point network security access policy violations and malicious (or inadvertent) network parameter misconfigurations resulting in security vulnerabilities.

NI-DEFENDER protects today's networks and is an enabler for those already moving to next generation NFV and SDN network paradigms.

Eliminate service outages and degradations caused by network security breaches

Neutralize insider threats, secure 3rd party access, and minimize security operations costs.

Eliminate risks from new technologies such as SDN and NFV

Assign privileges by role, location, time: supports fine grain role and attribute-based access control policies