Executive Summary

Nokia NetGuard Identity and Access Manager
Product introduction - Identity and Access Manager

Nokia’s NetGuard Identity Access Manager (IAM) is an industry proven solution trusted to protect some of the world’s most important networks. Spanning traditional Information Technology (IT) and Operational Technology (OT) environments, it provides customers a future-proof investment. While there are several enterprise-grade privileged access management solutions available in the industry, it is important to select a solution proven to be effective in the complex IT environment of service providers. A solution must seamlessly span IT systems (e.g. applications, databases) as well as OT systems (e.g. radio access networks, mobile core, IP networks), while supporting a heterogenous mix of applications and devices. Many solutions simply do not scale to meet the needs of the complex environments of most communication service providers.

NetGuard IAM allows security administrators to implement a single user interface to control, audit and manage all access to IT applications, physical and virtual network functions, as well as OSS/BSS/NMS/EMS, and other systems in the network. With flexible user access privileges to network functions and management systems, NetGuard IAM enables network administrators to manage and enforce network-wide security policies more effectively while reducing operating cost, time and effort. Furthermore, the product’s integrated Identity Access Governance module enables administrators to automate the access approval workflow, eliminating the often costly integration with 3rd party systems. The NetGuard IAM’s built-in workflow engine can be used to process access requests and approvals leveraging the product’s substantive REST API. Full workflow automation allows authorized application owners to review, approve or deny access permission permissions.

Scale and performance

Nokia’s solution is routinely used in networks supporting tens-of-thousands of users connecting to hundreds-of-thousands of target systems. Designed for scalability, to match the performance requirements for large scale implementations. Unlike appliance based solutions, NetGuard IAM supports clustering, enabling new virtual machines (VMs) to be added to existing implementations, allowing graceful expansion as the number of users or targets grows.

Agentless operation enables sophisticated capabilities

Nokia NetGuard IAM does not require any software agent to be installed on end-user client computers or target systems. The solution implements a proxy architecture. For CLI connections, users can proxy directly from end-user machines using any arbitrary terminal emulator (e.g. putty, secureCRT, etc.). For EMS/OSS/GUI applications, users connect to a Windows RDS server where the IAM client is located. This architecture ensures no client or special configuration in the web browser needed on end-user machines. It also ensures that video logging only captures user interactions with network devices from a centralized locked down Windows RDS server. This architecture simplifies the integration of additional target systems – whether IT web applications, network elements or complex graphical user interfaces – used to manage OT systems like BSS, OSS, NMS and EMS. This proxy architecture ensures that target element passwords are not subjected to the end-users, enabling additional security best practices.

NetGuard IAM’s architecture provides several additional benefits including full video and command line logging. The solution uses industry standard codecs enabling playback from any video player. NetGuard IAM administrators can play back video through the thin client admin console. Video search capabilities for embedded keystrokes is supported for native Windows applications, and this capability continues to be enhanced with subsequent product releases. NetGuard IAM supports live mirroring of both GUI and CLI sessions so administrators can view the activities of a session in real-time.
NetGuard IAM also provides real-time monitoring of user activity (individual or group level) with the ability to terminate a session immediately at the direction of an administrator, or the session can expire after a period defined by an administrator.

The solution supports role and attribute based access control, enabling flexible privilege segregation while also supporting privilege escalation.

Furthermore, it provides command filtering and restriction capabilities, offering administrators fine-grained control over what specific commands individual users, regardless of privilege, may execute on a target system. NetGuard IAM can be configured to send an alert or notification to an administrator when a prohibited command is attempted.

**Easy integration into heterogeneous environments**

Nokia customers routinely integrate NetGuard IAM with a variety of IT support systems. For instance, the solution supports SOAP/REST APIs that enable new targets to be easily included in existing systems. NetGuard has been successfully integrated into Security Information Event Management Systems (SIEM) enabling IAM logs to be collected, aggregated and correlated for alert and notification capabilities.

**Easy to develop application connectors**

Application connectors for NetGuard IAM can be easily developed. Nokia provides a software development kit (SDK) which includes development environment and test workbench allowing developers to build and unit test connectors. This enables new applications to be onboarded rapidly and fine-tuned to a customer’s specific environment.

NetGuard IAM supports adapters which provide more advanced and sophisticated capabilities including full credential management and password rotation on target systems, for instance, network elements such as routers, firewalls, mobile packet core, IMS, etc.

Some examples include, but are not limited to:

- Operating Systems: Windows, Linux/UNIX, Solaris, HP Unix, AIX, Mac OS
- Windows Applications: Service accounts including SQL server service accounts in cluster, Scheduled Tasks, IIS Application Pools, COM+, IIS Anonymous Access
- Web Applications commonly found in IT applications: SharePoint, Concur, Confluence, Jira
- Databases: Oracle, MSSQL, DB2, Informix, Sybase, any ODBC compliant database
- Security Appliances: CheckPoint, Nokia, Juniper, Cisco, Blue Coat, IBM, TippingPoint, SourceFire, Fortinet, WatchGuard
- Network Devices: Cisco, Juniper, Nortel, HP, 3com, F5, Alcatel
- Applications: SAP, WebSphere, WebLogic, JBOSS, Tomcat, Oracle ERP
- Directories: Microsoft, Sun, Novell, UNIX vendors
Suggested live integrated demonstrations

- Access to OT systems such as telecom network elements from vendors such as Huawei, ZTE, Nokia, Ericsson, using Telnet, SSH, FTP, and SFTP
- Provide controlled launch and single sign-on for OT EMS/NMS/OSS/BSS such as:
  - Huawei M2000, U2000
  - Nokia NetAct, 5620 SAM
  - ZTE NetNumen
  - Ericsson SDP manager, OCC, and EMM
- Demonstrate identity governance workflow process management, showing how an end-user can request additional or elevated access to network resources or systems, without having to use an external governance tool such as SailPoint
- Allow a user to “elevate” privileges to “root” either permanently within a prescribed time window, or temporarily without disclosure of root credentials to the given user
- Demonstrate time-based access controls by defining a user access as permanent, temporary for one or more specified time periods, or “one time” for one occasion only
- Provide single sign-on using generic terminal emulators, and not thin-clients
- Integrate into common or proprietary access tools like PuTTY, KiTTY, SecureCRT and Ericsson WinFiol
- Create blacklists and whitelists to enforce what commands a user is permitted to execute on a target system
- Demonstrate support for any internet browser
- Perform password rotation on element management systems such as Nokia NetAct and 5620 SAM
- Perform password rotation on a telecom network element from Nokia, Huawei, ZTE, Ericsson, Cisco, Juniper
- Manage and create user credentials on end-systems
- Demonstrate access for both physical and virtualized network devices (e.g. VNFs, SDN controllers, VIMs and orchestrators)
- Audit and identify misconfigurations of parameters on end systems en masse, and correlate those misconfigurations to specific users and sessions
- Discover unauthorized or rogue credentials on end-systems
The NetGuard security portfolio

NetGuard IAM is part of Nokia's comprehensive security portfolio. Unlike other suppliers of privileged access management solutions, Nokia provides a comprehensive solution helping customers navigate the increasingly challenging security landscape.

Service providers face growing security threats from cyber attacks to insider threats and misconfigurations. Breaches may result from inadvertent or malicious intentions against networks, either leveraging existing security holes or creating new ones.

Advanced Persistent Threats (APTs) are some of the most difficult to detect and often have the most significant consequences. APTs typically leverage undetected network access, using privileged access credentials and manipulated network security configuration policies. The outcomes could be data theft, monetary gain, or service disruption to name but a few. In one case, a service provider’s network was infiltrated to conduct espionage over an extended period. In another case, the motivation was financial gain achieved by modifying billing records.

Configuration errors enable 65 percent of security attacks and cause 62 percent of infrastructure downtime according to industry studies. Inadvertent or intentional insider misuse is behind 70 percent of all breaches. Most operators do not correlate the relationship between malicious attacks and outages. Sometimes incorrect configurations are introduced already at the time of installation and turn up. This delays service introductions, impacts revenue and profitability. Misconfigurations range from complex to mundane, including incorrect port configurations, location information, or bandwidth profiles.
In complex service provider environments, such as IMS, simple tasks like changing default passwords or rotating passwords, become cumbersome. As networks change and expand, network operators find it challenging to respond to business priorities that require frequent configuration changes. Potential for error increases dramatically.

A simple error in configuration could inflict serious security vulnerabilities. Typically, there is no way to control access device configurations based on user role, and checking or preventing unauthorized configuration changes is problematic. When something goes wrong whether due to faulty configuration or a security breach, it is hardly possible to trace the actions to an individual in the absence of audit trails.

NetGuard IAM can be used in combination with other NetGuard products to enrich capabilities in monitoring, mitigation and detection challenges. NetGuard helps to prevent threats before they materialize by rapidly spotting and stopping suspicious behavior, and automating responses to security events.

NetGuard Security Management Center (SMC) is an easy-to-use security orchestration, analytics and response solution that enables operators to prevent, pinpoint, and address security threats before they result in breaches. NetGuard SMC aggregates, analyzes and enriches security data from a variety of sources to help security and network operations teams assess business risks, improve decision making, and better control costs.

NetGuard SMC provides reporting, analytics and alerting using data from other NetGuard products as well as third parties. The out-of-the-box interactive dashboards can be modified to suit the operator’s unique needs.

NetGuard SMC provides the ability to proactively alert users to specific violations or detected threats, enabling rapid, immediate responses. SMC Smart Insights helps to detect important security events, helping security professionals to focus on key issues and risks. Combined with analytics, alerts provide a prioritized view of issues and risks.
The NetGuard Audit Compliance Manager (ACM) audits multi-vendor, hybrid, heterogeneous networks for incorrect or outdated configurations, and errors opening vulnerabilities. ACM ensures network security policies are correct and stay correct, simplifying the management of complex configuration compliance templates, accelerating network and service deployments.

Audit Compliance Manager Analytics
NetGuard Endpoint Security (NES) is a network based malware detection solution that identifies command-and-control data patterns of infected systems or endpoints, before malware or ransomware is detonated. NES is agentless, and does not require any special software to be installed on client devices. NES identifies the specific threat vector and helps security teams identify the endpoints that might be infected with malware such as keyloggers or ransomware.

Proven and trusted solution protecting the world’s most important networks
The Nokia NetGuard Identity and Access Manager is used by some of the world’s leading telecommunications companies including Telefónica, AT&T, AT&T Mexico, Vodafone, and Bell Canada. In a competitive market, many suppliers invest in promotion, sponsoring and advertising, instead, Nokia focuses on developing solutions that solve our customers’ key challenges. Our customers use NetGuard IAM to support user access management and governance in both IT and OT environments, providing the best total cost of ownership by using a single solution.
NetGuard Active security automates responses with cognitive analytics and threat intelligence

The NetGuard ACTIVE Security architecture leverages the unique capabilities of the NetGuard portfolio. The fusion of these capabilities into a cohesive, modular end-to-end solution which provides open interfaces for multi-vendor integration, delivers market differentiating capabilities, enabling service providers address the growing threat landscape resulting from mobile broadband expansion, IoT, Cloud and other technology disruptions.

It delivers reporting capabilities and real-time monitoring to provide contextual security issues alerts that help to reduce attack surface and time.