NOKIA

Compliance Awareness, Process Automation, and Intelligent Response

Challenges

Report preparation using data from multiple systems for a security audit can significantly increase a team's workload for weeks or even months. That's because detecting and monitoring compliance violations has become increasingly difficult in complex, multi-vendor environments spanning different types of networks and technologies. Tracking changes, authorization flows, and access controls, as well as the trails of who did what and when — comprehensively and reliably — requires time and effort and is undeniably prone to human mistakes and malicious behaviors. Having visibility of the security posture of the critical infrastructure of a growing network and being able to measure actual risks requires the real-time assessment of critical KPIs, as well as quick reaction to identified deviations.

What, then, are the critical components of a solution to address these challenges?

The solution

Automated regulatory compliance

To begin with, the solution needs to automate the audit and analysis of all the parameters in the physical and virtual networks. The Nokia NetGuard Audit Compliance Manager can be integrated into existing control databases and ticketing systems to centrally track all changes, required authorizations, as well as log and report them. The Audit Compliance Manager provides a complete audit trail against actual baseline values for each monitored device. By means of continuous and real-time scans of device parameters, the NetGuard Audit Compliance Manager can generate all required compliance reports, efficiently and automatically. Furthermore, it is highly flexible and supports a rich set of features to address any vendor's audit criteria.

Nokia NetGuard Audit Compliance Manager

Unified identity and access management

Second, the solution must provide unified identity and access management with single sign-on and centralized policies across multi-vendor, multi-technology networks and applications. The Nokia NetGuard Identity Access Manager is a single application that can be seamlessly integrated with existing identity management systems to automate and centrally manage passwords across all physical or virtual network functions. As a result, policies, such as Role Based Access Control (RBAC), can be automated by centrally defining roles, privileges, and controlling access or the password aging policy across a multitude of devices. This approach also prevents the need for shared accounts in order to jump hosts for access to older assets. Instead, many-to-one account mapping is used to manage access to these assets that support only a single user and password. The Nokia NetGuard Identity Access Manager provides comprehensive audit trails with logging and user activity replay, addressing regulatory and compliance reporting requirements, as well as forensic investigations.

Nokia NetGuard Identity Access Manager

Anomaly detection to protect industrial devices

Third, the solution must protect industry-specific devices, which have limited or no security capabilities, such as Remote Terminal Units (RTUs). It must meet this challenge by using deep analytics that monitor and analyze traffic, as well as search for patterns consistent with malware behavior, protocol anomalies, and deviations from normal traffic profiles. Nokia NetGuard Endpoint Security monitors traffic and compares it to baseline values. Reports of anomalies automatically generate alerts to initiate an appropriate response to conduct forensics or stop the traffic completely.

Nokia NetGuard Endpoint Security

Enhanced situational awareness and actionable compliance insights

Fourth, the solution must use data analytics to prevent, pinpoint, and address security threats before they result in breaches. The Nokia NetGuard Security Management Center (SMC) integrates and correlates data from existing security systems, as well as from those that lack single dashboard management platforms. This approach helps to assess business risks, improve quality of decision making, and overall response time to reduce potential recovery costs. It also includes integrating policy violations from the NetGuard Identity Access Manager and tracking changes identified by the NetGuard Audit Compliance Manager — changes, which are consistent with, or an exception to the baseline. The Security Management Center also correlates critical information, such as traffic anomalies, detected by NetGuard Endpoint Security, which enables the identification of potential attacks, as well as defective or misconfigured devices. This process also helps the analyst to investigate root causes and protect facilities effectively. Moreover, its analytics and reporting capabilities improve situational awareness and operational efficiency by automating and guiding responses to threats.

Nokia NetGuard Security Management Center

Why Nokia NetGuard

The Nokia NetGuard Security solution for utilities combines unified identity and access control with trailing of user activities, automated auditing of network parameters with centralized management of baselines, and powerful traffic and data analytics from multiple sources, using a single pane of glass perspective. The solution also automates and improves situational awareness, guides threat responses, and simplifies reporting for regulatory compliance for utilities today that have a growing cyberattack surface.

Nokia Oyj
Karaportti 3
FI-02610 Espoo, Finland
Tel. +358 (0) 10 44 88 000

Document code: SR1803024011EN (April)