MAY CYBER TECHNOLOGY

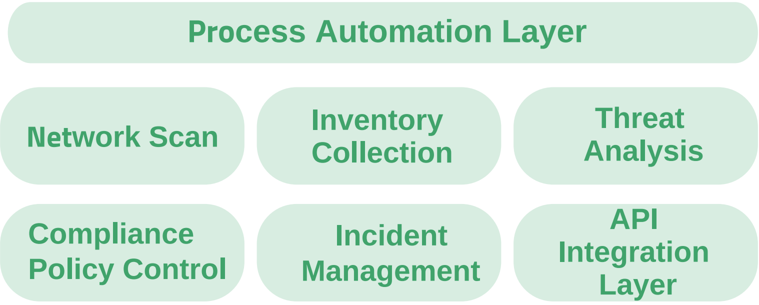
›SCOP NET

The inclusion of uncontrollable or unauthorized devices into corporate networks raises major risks. These devices can lead to unauthorized access toinformation, harm to computer network, and cause critical information to be captured by unauthorized persons. ScopNET is a solution that prevents unauthorized access to computer networks, detects malware with advanced threat analysis and has no dependency on 802.1x.

PROMINENT FEATURES

- **Infrastructure Control**
  Authentication and authorization is performed for devices within the wireless-wired-VPN networks.
- **Threat Detection for Critical Systems**
  Threats targeting the critical systems are identified through the monitoring of the end-user devices and networks.
- **Visibility on Network**
  The system collects the inventory of Windows/MAC/Linux computers and network devices, and analyzes this information.
- **Low Cost**
  The potential workload is prevented with brand-independent manageable switch support, agent-free architecture option, and architecture alternative that are not dependent on 802.1.
- **Manageable BYOD Strategy Creation**
  Provides BYOD management, which makes network management difficult for many organizations. BYOD strategy can be easily implemented with ScopNET.
- **Easy Implementation, Easy Management**
  ScopNET can perform detection and prevention operations by using multiple methods without requiring any changes to the network.

MODULES



Process Automation Layer

Network Scan

Inventory Collection

Threat Analysis

Compliance Policy Control

Incident Management

API Integration Layer

STRUCTURAL FEATURES

ScopNET offers different methods to authorize network access. The system can be integrated with routers, switching devices and firewalls.

There is no need for software installation on end-user devices. All threat analyses and inventory collection operations can be performed without an agent. As it requires small modifications on corporate networks, ScopNet solution is easy to implement.

When a new device is included into the network, first a classification is performed. Windows WMI, Windows RPC, SNMP and SSH protocols are used for device classification. Windows, Linux and MAC operating systems are supported.

Captive-Portal structure offers a unique end-user experience. A restricted network access can be granted to guest users via text message integration.

Malicious programs within the network are detected by advanced threat analysis. The security risks are identified through port scanning, weak password use and analysis of security event logs

MAY
CYBER
TECHNOLOGY

SCOP NET

IMPORTANT PRODUCT FEATURES

- 802.1x-independent architecture on network devices
- 802.1x support through included radius upon request
- Agent-free operation for Windows/MAC/ Linux operating system
- Ability to use different prevention methods to unauthorized access
- Automatic user registration for controlled access
- Architecture free from additional hardware/software for remote branch integration
- Integrated threat monitoring structure
- Integration with vulnerability scanning systems

THREAT ANALYSIS

- Classification of the applications using network port
- Classification of the applications creating
network traffic
- Bandwidth usage analysis
- Network traffic analytics
- Detection of port scanning
- Unauthorized username/password use
- Detection of weak SNMP passwords
Malicious program analysis

Ankara

ODTÜ Teknokent, Mustafa Kemal Mah.
Dumlupınar Bulvarı, 280/G Kat: 2,
06530
Çankaya - Ankara / Turkey
0 321 227 05 09
0 312 227 05 75

İstanbul

Maslak Mah. AOS 55. Sk. 42
Maslak Sitesi No:4
B Ofis Kat:8
Sarıyer / İstanbul
0 212 283 00 46
0 212 283 00 47

GENERAL FEATURES

- Agent-free architecture
- Ability to use different methods to prevent network access for a computer
  - Switch port VLAN changing
  - ACL management
  - Switch port closing
- Ability to use any information for security verification through WMI or remote log file access
- Central management and distribution
- Distributed architecture support
- Web-based interface
- Detailed reporting
- Captive-Portal for guest user management
- Planned/instant batch command sending to network devices
- API integration with security platforms
- Detailed network scan for device classification
- Access authorization in network devices with TACACS+ feature
- VPN Support
- Integration with Vulnerability Scanning Tools (Nesus)

DIFFICULTIES IN NETWORK ACCESS CONTROL

Guest User Access: The authorization and controlled inclusion to the network of guest users visiting the organizations for various reasons is a major problem. This access request can be made by a contracting company visiting for support or by a privileged guest.

Increased Mobile Device Use: The increase in the rates of employees using their mobile devices in the corporate network is the common problem of organizations. Everyday more and more users request access to corporate resources through their mobile devices.

Threats Targeting Critical Systems: The attacks on critical systems cause increased internal network usage. Protecting the systems against attacks is much more difficult due to the different access requirement within the internal network.

Compliance Requirements: Every standard about IT security aims to grant correct levels of authorization and setup an effective control infrastructure. Access control is a major problem for complex and distributed networks.

Heterogeneous & Distributed Network Infrastructure: VThe use of NAC solutions gained more importance with the increased number of VPN users, wireless network users, and endpoints. The traditional NAC solutions require 802.1x support and creates workload for network administrators due to the changes to be made on the network.

Therefore, many organizations only deploy NAC application in their central offices.